NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

INTEGRATION OF BEHAVIORAL THREAT MANAGEMENT INTO FUSION CENTER OPERATIONS TO PREVENT MASS OR TARGETED VIOLENCE

by

W. Payne Marks

December 2016

Thesis Advisor:	Robert Simeral
Second Reader:	Eugene Deisinger

Approved for public release. Distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

1. AGENCY USE ONLY ***(Leave blank)***

2. REPORT DATE
December 2016

3. REPORT TYPE AND DATES COVERED
Master's thesis

4. TITLE AND SUBTITLE
INTEGRATION OF BEHAVIORAL THREAT MANAGEMENT INTO FUSION CENTER OPERATIONS TO PREVENT MASS OR TARGETED VIOLENCE

5. FUNDING NUMBERS

6. AUTHOR(S) W. Payne Marks

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB number 2017.0029-DD-N.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release. Distribution is unlimited.

12b. DISTRIBUTION CODE

13. ABSTRACT (maximum 200 words)

Incidents of mass or targeted violence seem to occur without warning and lead us to conclude that nothing may be done to prevent them. These incidents may take the forms of mass shootings, stabbings, vehicular attacks, and other methods designed to kill or injure many people. Opportunities to detect and interdict potential attackers may exist. The literature identifies a host of warning behaviors that may be useful in detecting and disrupting acts of violence. This thesis examines the opportunities available to the nation's 78 fusion centers to help prevent mass or targeted violence by learning to conduct behavioral threat assessments and management activities. Analysis of four police agencies that conduct behavioral threat assessments is conducted. Also, the National Network of Fusion Centers is explored to determine whether behavioral threat assessment and management may be a good tool to incorporate into current violence prevention efforts. It was found that fusion centers already perform basic behavioral analysis through the vetting of suspicious activity reports as part of the Nationwide Suspicious Activity Reporting Initiative. Preventive efforts may be more successful should principles of behavioral threat assessment and management be incorporated into fusion center operations.

14. SUBJECT TERMS
threat assessment, behavioral threat assessment, behavioral threat management, warning behaviors, violence prevention, suspicious activity reporting, fusion centers

15. NUMBER OF PAGES
115

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT
Unclassified

18. SECURITY CLASSIFICATION OF THIS PAGE
Unclassified

19. SECURITY CLASSIFICATION OF ABSTRACT
Unclassified

20. LIMITATION OF ABSTRACT
UU

THIS PAGE INTENTIONALLY LEFT BLANK

INTEGRATION OF BEHAVIORAL THREAT MANAGEMENT INTO FUSION CENTER OPERATIONS TO PREVENT MASS OR TARGETED VIOLENCE

W. Payne Marks
Lieutenant, Virginia State Police, Richmond, Virginia
B.S., University of Mary Washington (formerly Mary Washington College), 1992

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)

from the

NAVAL POSTGRADUATE SCHOOL
December 2016

Approved by: Robert Simeral
Thesis Advisor

Eugene Deisinger
Second Reader

Erik Dahl
Associate Chair for Instruction
Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Incidents of mass or targeted violence seem to occur without warning and lead us to conclude that nothing may be done to prevent them. These incidents may take the forms of mass shootings, stabbings, vehicular attacks, and other methods designed to kill or injure many people. Opportunities to detect and interdict potential attackers may exist. The literature identifies a host of warning behaviors that may be useful in detecting and disrupting acts of violence. This thesis examines the opportunities available to the nation's 78 fusion centers to help prevent mass or targeted violence by learning to conduct behavioral threat assessments and management activities. Analysis of four police agencies that conduct behavioral threat assessments is conducted. Also, the National Network of Fusion Centers is explored to determine whether behavioral threat assessment and management may be a good tool to incorporate into current violence prevention efforts. It was found that fusion centers already perform basic behavioral analysis through the vetting of suspicious activity reports as part of the Nationwide Suspicious Activity Reporting Initiative. Preventive efforts may be more successful should principles of behavioral threat assessment and management be incorporated into fusion center operations.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ASU	Analytical Support Unit
ATAP	Association of Threat Assessment Professionals
BAU	Behavioral Analysis Unit
CTTWG	Counter-Terrorism Training Coordination Working Group
DHS	Department of Homeland Security
ECSP	Exceptional Case Study Project
FBI	Federal Bureau of Investigation
GEOINT	geospatial intelligence
GIWG	Global Intelligence Working Group
HUMINT	human intelligence
IC&Cs	Inappropriate Communications or Contacts
ISIS	Islamic State in Iraq and Syria
JTTF	Joint Terrorism Task Force
LAPD	Los Angeles Police Department
NCISP	National Criminal Intelligence Sharing Plan
NJ ROIC	New Jersey Regional Operations Intelligence Center
NSI-SAR	Nationwide Suspicious Activity Reporting Initiative
OMG	outlaw motorcycle gang
OSINT	open source intelligence
SAR	suspicious activity report
SIGINT	signals intelligence
SNA	social network analysis
START	Study of Terrorism and Responses to Terrorism
TAS	Threat Assessment Section
TAT	threat assessment team
TMU	Threat Management Unit
USCP	United States Capitol Police
USMS	United States Marshals Service
USSS	United States Secret Service
VFC	Virginia Fusion Center

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I wish to thank my thesis committee, Captain Robert Simeral (United States Navy, Retired), and Dr. Eugene Deisinger, for their patience and guidance as the project unfolded. Each offered unique insight that helped to see this effort through.

I also wish to thank Colonel W. Steven Flaherty, superintendent of the Virginia State Police, for the leadership he has provided to my organization over the years and the support he has given to his personnel who have pursued the educational opportunities offered by the Naval Postgraduate School’s Center for Homeland Defense and Security. This commitment reaps benefits for the Virginia State Police, but more importantly, for the greater homeland security enterprise of our country.

My gratitude is also extended to Lieutenant Colonel Rick A. Jenkins, Major Gary T. Settle, and Captain Steven W. Lambert of the Virginia State Police Bureau of Criminal Investigation for the significant support and encouragement provided by each.

Special thanks also go to Mr. Robert W. Reese, lead intelligence analyst with the Virginia Fusion Center. Mr. Reese’s vision and passion for behavioral threat assessment and management sparked my interest in this topic. His insight and leadership in this area is groundbreaking for fusion centers and opportunities to prevent violence and save lives.

My thanks are also extended to the men and women of the Virginia Fusion Center. I am proud to serve with you all as we strive to make our contribution to the security of our state and country. While humble professionals, this group of analysts and state police agents and supervisors truly make a positive difference for us all.

Finally, I wish to thank my wife, Monica, for her encouragement and the many sacrifices she made to allow my pursuit of this thesis and the educational program at the Center for Homeland Defense and Security. She, along with my parents, daughter, sister, and other family members, endured my frequent absences from many important gatherings over the last 18 months to attend to the work this program requires. Love and thanks to you all.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. PROBLEM STATEMENT

Violence pervades every aspect of contemporary life. Technological advancements and modernization have improved the quality and longevity of human life over many years, yet violence among humans remains a pervasive challenge. Today, this nation is troubled by what is conceptually coined *intended violence*, including workplace attacks, school shootings, public figure attacks, and hate crimes.[1]

Intended violence may also be regarded as *targeted* violence. Targeted violence is frequently reported in the American media and the term refers to actual or threatened acts of violence.[2] As with intended violence, examples include stalking, workplace violence, and attacks on public figures.[3]

Violence motivated by terrorism also remains a concern. Recent examples from western countries include mass shootings in Orlando, Florida; San Bernardino, California; Paris, France; and bombing attacks in Brussels, Belgium.

Much has been written about the causes of violence. Arguments are made that violence is properly regarded as a public health problem and should be treated as a disease, or that violence is a learned behavior with an environmental nexus, or that violence stems from social problems, such as poverty, disease, discrimination, or educational failures.[4] Others posit that violence is the result of flaws in American culture, overly aggressive parenting, the presence of firearms in U.S. society, the result of playing violent video games, or observing violent television programs or movies.[5] Yet, the historical record shows that violence among humans has existed over the millennia,

[1] Frederick Calhoun and Stephen Weston, *Contemporary Threat Management* (San Diego, CA: Specialized Training Services, 2003), 16.

[2] Robert A. Fein, Bryan Vossekuil, and Gwen A. Holden, *Threat Assessment: An Approach to Prevent Targeted Violence* (Washington, DC: National Institute of Justice, 1995), 1.

[3] Ibid., 2.

[4] Steven Pinker, *The Blank Slate-The Modern Denial of Human Nature* (New York: Penguin Putnam, Inc., 2002), 308, 312–313.

[5] Ibid., 308–309, 311.

before the presence of firearms, America, violent media, educational systems, and other contemporary variables.[6]

Roger Depue, former head of the FBI Behavioral Analysis Unit (BAU), makes a similar observation in his book entitled *Between Good and Evil*. Depue ponders the nature of evil within humans and how the emergence of serial killers had occurred. Historically, he points out, such a phenomenon was often attributed to the same causes as those noted previously, such as societal factors, American culture, and so on.[7] Depue then offers examples from history, such as a 15th century figure by the name of Gilles de Rais, who sadistically murdered 800 children,[8] or how in London, Jack the Ripper attacked and disemboweled at least six women in 1888.[9] Each of these examples preceded modern times, modern technology, the influence of violent media, or exposure to American culture.

While much of Depue's work pertains to the criminal investigations of serial murderers, rapists, and the crimes they have committed, lessons can be applied from his specialty to the field known as behavioral threat assessment. As covered in greater detail later, Depue was perhaps the first to use the term *leakage* to describe the process by which killers or attackers reveal or "leak" information during communications to others about their motivations, fantasies, and intentions.[10] The concept of leakage is important to those investigating homicides that have already occurred, but may be of greater value for threat assessors and managers attempting to prevent violence. Additional so-called warning behaviors exist in addition to leakage that serve threat assessors and managers addressed later in this thesis. Detecting and making use of subtle behavioral indicators, such as *leakage* may offer hope to prevent violence rather than investigate it after it has occurred.

[6] Pinker, *The Blank Slate-The Modern Denial of Human Nature*, 306.

[7] Roger L. Depue and Susan Schindehette, *Between Good and Evil* (New York: Time Warner Group, 2005), 158.

[8] Ibid.

[9] Ibid.

[10] Ibid., 155.

Writing in *The Blank Slate—The Modern Denial of Human Nature,* Steven Pinker quotes Winston Churchill, who offered this assessment of humanity, "The story of the human race is war. Except for brief and precarious interludes there has never been peace in the world; and long before history began murderous strife was universal and unending."[11]

Pinker notes Churchill's dim assessment of human nature and makes the case that violence is best understood through study of the human mind.[12] Psychological study of violence and those who may engage in violence is not a simple undertaking. Behavioral threat assessment expert J. Reid Meloy cautions that when attempting to evaluate the risk for violence in a person, it is crucial to recognize two things. First, people will always know less than they think they do about the person of our concern.[13] Second, mental health services cannot repair all abnormal human behaviors.[14]

Where does this leave everyone? If violence is a natural condition of human nature as Pinker argues, and if knowledge of people is limited and some people are unable to be steered away from a violent decision by mental health professionals as Meloy warns, how can the terrible instances of violence plaguing this nation be prevented?

Over time, the effort to understand and prevent violence has been attempted by academics and practitioners. This thesis focuses on a process known as behavioral threat assessment and management. Organizations successfully utilizing behavioral threat assessment and management are explored. It also explores the opportunities that may exist to leverage some or all of the nation's 78 fusion centers to prevent violence by facilitating behavioral threat assessments and developing threat management strategies. Through established programs, such as the Nationwide Suspicious Activity Reporting Initiative (NSI-SAR), use of the intelligence cycle, and conducting all-hazards

[11] Pinker, *The Blank Slate-The Modern Denial of Human Nature,* 306.

[12] Ibid., 317.

[13] J. Reid Meloy, *Violence Risk and Threat Assessment* (San Diego, CA: Specialized Training Services, 2000), 3.

[14] Ibid.

intelligence analysis, fusion centers are already incorporating behavioral criteria into their analytic and informative processes.[15] Considering the opportunities to prevent violence through behavioral threat assessment and management, an analysis of the process and potential for use by fusion centers is in order. Finally, policies currently in use by other organizations are considered for use in fusion centers to contribute to the larger effort to prevent violence.

The purpose of this thesis is to explore the opportunities for the nation’s fusion centers to augment efforts to prevent mass or targeted violence by utilizing the principles of behavioral threat assessment and management. Mass violence and murder resulting from terrorist attacks, school shootings, stalking, and other tactics presents exceptional challenges for public safety officials. The evolution of fusion centers to include all hazards-all crimes priorities has created greater utility and greater opportunities to serve local, state, and federal law enforcement and public safety partners. Building on the behavioral analysis that accompanied the NSI-SAR may augment the impact of fusion centers to prevent violence and other crimes. Specifically, the incorporation of the principles of behavioral threat assessment and management by fusion centers may lead to the disruption and prevention of a host of violent acts that would otherwise have occurred.

B. RESEARCH QUESTIONS

Behavioral threat assessment and management is a process that has been successfully utilized by many organizations, including the Los Angeles Police Department (LAPD), the United States Capital Police (USCP), the United States Marshals Service (USMS), and the United States Secret Service (USSS). It is also in use by many of the nation’s colleges and universities to mitigate threats that arise at educational institutions. Can this process also be used by the nation’s fusion centers to prevent mass or targeted violence? If so, what adaptations to the process may be required for fusion centers to make positive use of it? What may be learned and applied from those

[15] “Nationwide SAR Initiative (NSI)—About the NSI,” accessed July 24, 2016, https://nsi.ncirc.gov/about_nsi.aspx.

who employ the behavioral threat assessment and management methodology for the purpose of violence prevention?

THIS PAGE INTENTIONALLY LEFT BLANK

II. LITERATURE REVIEW

Three sub-literatures provide the foundation upon which the research in this thesis is conducted, violence and threat typology, responses to violence, and the prevention of violence. The prevention category includes historic responses to violence, legislation, tactics, and preventive measures. Among the preventive measures are fusion center operations, the NSI-SAR, behavioral threat management and the organizations that employ this method for violence prevention.

A. VIOLENCE AND THREAT TYPOLOGY

Incidents of unforeseen violence present exceptional challenges to security services and the public. Examples include active shooters motivated by political or religious ideologies or those afflicted with mental illness or other personal concerns. According to the Federal Bureau of Investigation (FBI), the term "active shooter is used by law enforcement to describe a situation in which a shooting is in progress and an aspect of the crime may affect the protocols used in responding to and reacting at the scene of the incident."[16] Further, to label a shooting as "active" means that the circumstances of such an incident may be affected by police responders or even citizens, depending upon the circumstances.[17] Since 70% of active shooting incidents end in less than five minutes and 36% end in two minutes or less,[18] the public has been encouraged to consider its own counter-measures since a police response to an active shooter is often not fast enough to prevent loss of life. The FBI notes a publicly released 2013 video created by the Houston Mayor's Office of Public Safety and Homeland Security entitled "Run. Hide. Fight. Surviving an Active Shooter Incident"[19] that provides guidance to citizens regarding ways to protect themselves and others during an active shooting

[16] John Peterson Blair and Katherine W. Schweit, "A Study of Active Shooter Incidents, 2000–2013," University of Colorado at Boulder, 4, 2013, https://hazdoc.colorado.edu/handle/10590/2712.

[17] Ibid.

[18] Ibid., 8.

[19] "Run. Hide. Fight. Surviving an Active Shooter Event," video, 2013, https://www.fbi.gov/about-us/cirg/active-shooter-and-mass-casualty-incidents/run-hide-fight-video.

incident. The video portrays a fictional active shooting incident in an urban setting and the reactions of those affected.[20] It illustrates the vulnerability of people when faced with an active shooter. Concluding its 2013 analysis of active shooter incidents between 2000 and 2013, the FBI reported that avoidance of active shooter tragedies is the best outcome, adding that prevention efforts within all affected communities are critical.[21] The need to identify active shooter prevention measures and prevention strategies for other forms of violence thus contributes to this literature review. Research exists that explores techniques by which assessments of potentially violent behavior may be accomplished, such as the use of social media by terror organizations to recruit followers to commit mass murder, and opportunities to use social media to disrupt the pervasive gang violence occurring across the United States.

Targeted violence is not exclusive to active shooters or incidents of mass murder perpetuated by those afflicted with mental illness. Violence also occurs via gang conflict, terrorism, domestic disputes, and other crimes. The Association of Threat Assessment Professionals (ATAP) studies violence and works with public and private organizations to help prevent violence by sharing information, research, and practices with others in need of guidance regarding threat management.[22]

Research is evolving and growing as it pertains to violent incidents, indicators of pending violence, threat assessment protocols, and techniques by which to study or prevent violence. Threats of violence are diverse. However, opportunities to detect and possibly prevent violent acts exist, which is reflected in the diversity of literature available on this topic. For example, the rapidly developing realm of social media has lead to a host of new studies concerning the numerous variables that may contribute or prevent violence. Understanding the impact of social media on the opportunities to detect threats and mitigate them is important. However, the research also revealed the importance of developing a process by which threats may be detected, considered, and

[20] "Run. Hide. Fight. Surviving an Active Shooter Event."

[21] Blair and Schweit, "A Study of Active Shooter Incidents, 2000–2013," 21.

[22] "About ATAP," 2013, http://www.atapworldwide.org/?page=1.

handled. First, a discussion of the historic responses to violence is useful and follows in Part B.

B. RESPONSES TO VIOLENCE

Robert Fein, Bryan Vossekuil, and Gwen Holden, writing for the National Institute of Justice, observe that the traditional policing methods in use by American law enforcement has been reactive and designed to investigate and prosecute criminals after offenses have occurred.[23] Borum, Fein, Vossekuil, and Berglund, writing for the journal *Behavioral Sciences and the Law*, also note that the historic role of American law enforcement has been reactive, not preventive.[24] They go on to note that the expectations of law enforcement are evolving and that now, law enforcement and mental health providers are challenged with the ongoing needs to provide assessments pertaining to the potential for those who have previously engaged in violence police to repeat their acts, as well as the types of violence that may be carried out.[25]

C. PREVENTION OF VIOLENCE

1. Traditional Responses to Violence

Fein, Vossekuil, and Holden note that clearly articulated protocols or procedures are not currently in place among the larger law enforcement community.[26] Their study includes recommendations for establishing a threat assessment and management program. They go on to suggest that threat assessment is best accomplished by establishing a structured process or program by which those who pose a threat of violence may be identified, assessed, and managed in such a way that they are steered or guided away from a decision to carry out a violent act.[27] Building on this, Borum et al. note that police officers, workplace managers, school officials, and others are responsible for

[23] Fein, Vossekuil, and Holden, *Threat Assessment: An Approach to Prevent Targeted Violence*, 2.

[24] Randy Borum et al., “Threat Assessment: Defining an Approach for Evaluating Risk for Targeted Violence,” *Behavioral Sciences & the Law* 17, no. 3 (1999): 324.

[25] Ibid.

[26] Fein, Vossekuil, and Holden, *Threat Assessment: An Approach to Prevent Targeted Violence*, 3.

[27] Borum et al., “Threat Assessment: Defining an Approach for Evaluating Risk for Targeted Violence,” 326.

taking action upon receipt of potential threats in their organizations.[28] John Jarvis and J. Amber Sherer also recommend the utility of multi-disciplinary threat management efforts to improve the likelihood of successful prevention.[29] They note that law enforcement has embraced crime prevention programs over the years but threat management requires the input of stakeholders outside of the law enforcement community to ensure the broadest visibility and understanding of cases being managed.[30] Further, they add that a need exists for collaboration when conducting threat assessments. Continuing, Jarvis and Sherer claim that collaboration may help shift the traditional reactive culture of policing toward a more proactive approach; while also improving reporting from the community as a result of improved community relations.[31]

2. Prevention of Violence through Behavioral Threat Management

Andrew Harris and Arthur Lurigio, in the *Journal of Police Crisis Negotiations*, noting that law enforcement personnel are expected by the public to respond to threats of targeted violence, while balancing the need to protect civil liberties, also support this view.[32] They add that law enforcement must consider the adoption of new methods and skills coupled with changes in resource deployment.[33]

Building on this concept, Frederick Calhoun and Stephen Weston argue that threat assessment differs from traditional criminal investigations in that a logical conclusion is often elusive. Criminal cases conclude upon arrest and conviction of a perpetrator. Threat assessment cases do not' usually end this way. Often, an opportunity exists to arrest a suspect, but neither an arrest nor conviction necessarily reduces the need to manage the

[28] Borum et al., "Threat Assessment: Defining an Approach for Evaluating Risk for Targeted Violence," 324.

[29] John Jarvis and J. Amber Scherer, *Mass Victimization-Promising Avenues for Prevention* (Washington, DC: Federal Bureau of Investigation, 2015), 11.

[30] Ibid.

[31] Ibid., 4.

[32] Andrew J. Harris and Arthur J. Lurigio, "Threat Assessment and Law Enforcement Practice," *Journal of Police Crisis Negotiations* 12, no. 1 (May 2012): 52, doi: 10.1080/15332586.2012.645375.

[33] Ibid., 53.

threat, as incarceration allows for time to plan for violent action upon being released.[34] Calhoun and Weston argue that threat assessment is an ongoing process that requires diligent attention.

J. Reid Meloy and Mary Ellen O'Toole caution about the need to establish a process by which threat assessments may be accomplished, stating, "unstructured professional judgment relies on the notion of *ipsi dixit*, literally; 'he himself said it', and when translated into common parlance means the assessor knows it is true because he is the assessor and he knows best."[35] Thus, unstructured professional judgment is a poor tool by which to assess threats. Meloy and O'Toole, therefore, advocate for a process governed by structured professional judgment, whereby assessors evaluate threats based upon eight identified types of warning behaviors.[36]

Mary Ellen O'Toole and Sharon Smith wrote chapter 18 of the *International Handbook of Threat Assessment*. This chapter is focused upon documenting the fundamentals of threat assessment for beginners.[37] Regarding the necessity for specific processes, the authors note that it is important to define the purpose of a threat assessment program because doing so helps clarify the background and expertise of those who should be involved, their roles, how threats may be managed, and how strategies for intervention are developed.[38]

Andre Simons and Ronald Tunkel, writing chapter 12 of the book *International Handbook of Threat Assessment,* speak to the need to establish protocols by which assessments are made so that the quality of assessments may improve.[39] The authors

[34] Calhoun and Weston, *Contemporary Threat Management*, 266.

[35] J. Reid Meloy and Mary Ellen O'Toole, "The Concept of Leakage in Threat Assessment," *Behavioral Sciences & the Law* 29, no. 4 (July 2011): 514, doi: 10.1002/bsl.986.

[36] Ibid.

[37] Mary Ellen O'Toole and Sharon S. Smith, "Fundamentals of Threat Assessment for Beginners," in *International Handbook of Threat Assessment*, ed. J. Reid Meloy and Jens Hoffmann (New York: Oxford University Press, 2014), 272.

[38] Ibid., 274.

[39] Andre Simons and Ronald Tunkel, "The Assessment of Anonymous Threatening Communications," in *International Handbook of Threat Assessment*, ed. J. Reid Meloy and Jens Hoffmann (New York: Oxford University Press, 2014), 195.

provide commentary in this chapter about historical research conducted by the U.S. Secret Service and the joint Safe School Initiative coordinated by the U.S. Department of Education and U.S. Secret Service, which showed that offenders who committed targeted acts of violence rarely issued a directly-communicated threat to their intended target prior to attacking.[40] As members of the FBI Behavioral Analysis Unit, the authors describe the process by which threats are reported to a threat assessment team (TAT) for analysis.

Using a hybrid group of professionals and structured professional judgment approach to develop the analysis of threats fully, the TAT begins the process with a set of "triage questions."[41] Following this step, additional analysis unfolds regarding the mode of delivery of the threat, victimology and potential relationships between target and attacker, motive, veracity, resolution to commit violence, and imminence in threatening communications.[42] The TAT members then individually assess the threat and later combine their work into a team consensus followed with a written report.[43] Concluding, Simons and Tunkel note the process they use in the FBI's behavioral assessment unit represent only one methodology for evaluating anonymous threatening communications, adding that no single process will be adequate for all of the various circumstances with which threat assessors may be faced.[44]

3. Warning Behaviors and Threat Assessment

Fein, Vossekuil and Holden posit that violence is a process and often occurs as the culmination of identifiable problems, disputes, or conflicts that have developed over time.[45] Writing *Protective Intelligence and Threat Assessment Investigations*, Robert Fein and Bryan Vossekuil report "almost without exception, assassinations, attacks, and

[40] Simons and Tunkel, "The Assessment of Anonymous Threatening Communications," 195.

[41] Ibid., 199.

[42] Ibid., 208.

[43] Ibid., 209.

[44] Ibid., 210.

[45] Fein, Vossekuil, and Holden, *Threat Assessment: An Approach to Prevent Targeted Violence*, 3.

near-attacks are neither impulsive nor spontaneous acts."[46] Therefore, the literature suggests that opportunities exist for law enforcement and others to identify warning behaviors and utilize a threat management process to prevent violence from occurring.

Katie Cohen et al. discussed linguistic markers for radical violence in social media in a 2014 study within the journal *Terrorism and Political Violence*. They note that lone actor terrorism remains a marginal phenomenon compared to other acts of terrorism.[47] Nevertheless, cause for concern about this form of violence is growing because

> the capability threshold for individuals to carry out advanced attacks is becoming lower with time due to the power of the Internet to bring critical information, such as tutorials on bomb-making or geographical information, 'to your fingertips'. There is also concern that the Internet is making it easier than ever to engage in the study and dissemination of extremist views. Finally, a third reason is that many methods employed by security services and police to uncover and prevent group plots are of little use when the perpetrator is acting alone.[48]

This point leads to the possibility that a focused threat assessment process may help parse the contents of certain social media content to predict and stop violence before it occurs.

Building on this concept of assessment and intervention, Frederick Calhoun and Stephen Weston writing in their book, *Contemporary Threat Management: A Practical Guide of Identifying, Assessing, and Managing Individuals of Violent Intent*, articulate threat assessment principles that have been used by many professionals over the years to detect and prevent potential violence. Supported by case studies, the book posits that retroactive analysis of violent acts reveals noticeable behaviors that could have been detectable during the thinking, planning, preparing, and talking of a violent actor.[49] The authors also make the argument that a need exits for an established threat management

[46] Robert A. Fein and Bryan Vossekuil, *Protective Intelligence Threat Assessment Investigations* (Washington, DC: U.S. Department of Justice Office of Justice Programs, 1998), 16.

[47] Katie Cohen et al., "Detecting Linguistic Markers for Radical Violence in Social Media," *Terrorism and Political Violence* 26, no. 1 (January 2014): 246, doi: 10.1080/09546553.2014.849948.

[48] Ibid., 247.

[49] Frederick S. Calhoun and Stephen W. Weston, *A Practical Guide for Identifying, Assessing and Managing Individuals of Violent Intent* (San Diego, CA: Specialized Training Services, 2003), 23.

process for those professionals who endeavor to detect and disrupt violent action before it occurs.[50] This process is called behavioral threat management and rather than attempting to predict violence, it involves the creation of proactive procedures that allow law enforcement personnel or others to identify potential threats, assess and investigate them, and craft a plan to manage the threats to prevent violence.[51]

Written in 2003, *Contemporary Threat Management* preceded the rise of social media and its impact in current times. However, the material regarding the process by which threat assessments should be organized and conducted remains highly relevant and is routinely cited by researchers of follow-up works in more recent years. Important to social media communications, Calhoun and Weston discuss the concept of "hunters versus howlers."[52] This phrase pertains to the value of parsing and understanding communication that may not immediately be clear. The need to understand such communication is because hunters and howlers behave differently, hunters act and howlers talk.[53]

Meloy and O'Toole built on the work on Calhoun and Weston by noting ways in which a hunter or a howler might be detected in their 2011 study in the journal *Behavioral Sciences and the Law* entitled, "The Concept of Leakage in Threat Assessment."[54] Leakage in this context is defined as "communication to a third party of an intent to harm a target."[55] Leakage is further noted to be a form of warning behavior that "occurs in a majority of cases of attacks on and assassinations of public figures, adult mass murderers, adolescent mass murderers, and school or campus shootings: very low frequency, but catastrophic acts of intended and targeted violence."[56] Integrating the concepts of leakage with those of hunters vs. howlers helps determine whether language

[50] Calhoun and Stephen W. Weston, *A Practical Guide for Identifying, Assessing and Managing Individuals of Violent Intent*, 2.

[51] Ibid., 25.

[52] Ibid., 42.

[53] Ibid., 43.

[54] Meloy and O'Toole, "The Concept of Leakage in Threat Assessment," 513.

[55] Ibid.

[56] Ibid.

gleaned through social media may be representative of a true threat (from a hunter), or instead, menacing, but unlikely to lead to violence (from a howler). Meloy and O'Toole note that *leakage* is one of eight scientifically validated warning behaviors; the others being *pathway, fixation, identification, novel aggression, energy burst, directly communicated threat, and last resort*.[57]

Leakage is particularly important to this literature review, as it is the essence of the opportunity by which to use social media to detect someone who is on a pathway to violence. Meloy and O'Toole note that "among adult mass murderers who killed at least three people during one incident, the majority appear to leak their intent to third parties before they attack."[58] This leakage took the form of generalized (no location or victim pool identified) or mixed threats (generalized threat coupled with a specific threat).[59] It is useful to illustrate an example of a generalized threat, which could be, "I'm going hunting," while an example of a specific threat may be a suicide note describing a massacre in detail.[60]

It is also useful to consider an example of leakage and direct threats from adolescent mass murderers, who engage in both at rates higher than their adult counterparts.[61] A majority of mass murders do not directly threaten their targets; for example, "Tomorrow you find out if you live or die."[62] Leakage by mass adolescent mass murders is, "Wouldn't it be fun to kill all those jocks?"[63] These examples are taken from those who have committed mass murders, but do not address specific motivations of the killers.

Opportunities sometimes exist to detect leakage from someone about to engage in radical violence. Such violence is often associated with so-called lone wolf terrorism.

[57] Meloy and O'Toole, "The Concept of Leakage in Threat Assessment," 515.

[58] Ibid., 516.

[59] Ibid.

[60] Ibid.

[61] Ibid.

[62] Ibid.

[63] Ibid.

Cohen et al. added to the research concerning leakage through their 2014 study entitled "Detecting Linguistic Markers for Radical Violence in Social Media." They corroborate the work of Meloy and O'Toole by confirming the eight previously described warning behaviors, but add that searching for lone wolf terrorists is akin to "searching for a needle in a haystack."[64]

While Meloy and O'Toole focused on leakage, Cohen et al. also emphasized the importance of the behavior of *identification* as it applies to terrorists. This behavior is defined as one that indicates a

> desire to be a 'pseudo-commando', have a warrior mentality, closely associate with weapons or other military or law enforcement paraphernalia, identify with previous attackers or assassins, or identify oneself as an agent to advance a particular cause. Narcissistic ideas and fantasies about oneself are also counted in this group of warning behaviors.[65]

According to Cohen et al., "lone wolf terrorists and attackers of public figures often tend to identify themselves as a kind of warrior or person who is prone to use structured violence for a 'higher cause.'"[66] Further, it is suggested in this study that commonality exists among all attackers. Specifically, the authors note that it is common to find Internet-based videos or photos showing attackers posing with their weapons as if about to attack.[67]

4. Threat Assessment and Terrorist Threats

There are also implications for the counter-terrorism effort currently underway. Writing in *Studies in Conflict & International Terrorism*, Mohammed Hafez and Creighton Mullins discuss the terror threat from radicalized Muslims living in the West.[68] They point out that Western governments are under significant pressure to identify and

[64] Cohen et al., "Detecting Linguistic Markers for Radical Violence in Social Media," 247.

[65] Ibid., 249.

[66] Ibid.

[67] Ibid.

[68] Mohammed Hafez and Creighton Mullins, "The Radicalization Puzzle: A Theoretical Synthesis of Empirical Approaches to Homegrown Extremism," *Studies in Conflict & Terrorism* 38, no. 11 (November 2, 2015): 958, doi: 10.1080/1057610X.2015.1051375.

disrupt “budding terrorists” before they become fully radicalized.[69] Further, they note that analysts are taking on greater burdens due to the pressures of identifying the many variables that contribute to the process of radicalization by people who lead otherwise ordinary lifestyles.[70] They go on to identify cognitive radicalization (embracing ideas and political ideals outside of societal mainstreams) and behavioral radicalization (engaging in activities that may result in terrorism) while arguing that violence often, but not always, follows the combination of cognitive and behavioral radicalization in a person.[71]

Threat assessors may have opportunities to contribute to the effort of identifying the various pieces of the radicalization puzzle. According to Hafez and Mullins, the puzzle pieces include grievances, networks, ideologies, enabling environments, and support structures.[72] These elements are individually discussed in greater detail in the study. Social media analysis may be one avenue by which the elements of the puzzle may be observed.

Borum et al. discussing the process of threat assessment, argue that a conceptual approach to threat assessment has value because it does not require profiles based upon demographics or psychological traits.[73] Profiles are shown to be fruitless pursuits, superseded by the individualized process of threat assessment, which is based upon the unique variables influencing the circumstances. Fein and Vossekuil, in their work entitled, *Protective Intelligence and Threat Assessment Investigations*, add to this approach by observing that threat assessment also needs not utilize threats articulated verbally or in writing as risk thresholds.[74]

[69] Hafez and Mullins, “The Radicalization Puzzle: A Theoretical Synthesis of Empirical Approaches to Homegrown Extremism,” 958.

[70] Ibid.

[71] Ibid., 961.

[72] Ibid.

[73] Borum et al., “Threat Assessment: Defining an Approach for Evaluating Risk for Targeted Violence,” 327.

[74] Fein and Vossekuil, *Protective Intelligence Threat Assessment Investigations*, 15.

5. Threat Assessments and Mental Illness

Frequently, when considering an act of mass violence, friends, family, or professional investigators may spontaneously conclude that the attacker "just snapped" or spontaneously attacked due to mental illness.[75] The literature is not in full agreement as to the significance of mental illness as a factor in such cases. J. Reid Meloy, writing in the *Journal of Threat Assessment and Management* observes that when considering approaches and attacks of public figures, mental illness has a "substantial presence" in the analysis of the perpetrators.[76] Borum et al. contribute to this observation by stating that mental illness is not strongly associated with violence unless the variable of substance abuse is introduced to the equation.[77] This observation deals with the full range of violence and is not limited to analysis of mass targeted violence. However, Jarvis and Scherer assert that prevailing myths are associated with mental illness and mass victimization events and that they may be enhanced as a result of popular reactions that occur in the public sphere.[78] They note that data correlating mental illness with homicides is lacking and associated with two prevailing myths.[79] The first myth is that mentally ill persons are dangerous to others solely because of their mental illness.[80] While some forms of mental illness are associated with increased risk for violence, the authors point out that "not everyone who is a violence risk has a mental illness."[81] The second myth is that mentally ill persons must undergo a risk assessment for violence.[82] Thus, the authors point out that not all people afflicted with mental illness are likely to

[75] Chuck Tobin, "Message from the President: 25th Anniversary of the Association of Threat Assessment Professionals Annual Threat Management Conference," *Journal of Threat Assessment and Management* 2, no. 3–4 (2015): 229, doi: 10.1037/tam0000053.

[76] J. Reid Meloy, "Approaching and Attacking Public Figures: A Contemporary Analysis of Communications and Behavior," *Journal of Threat Assessment and Management* 1, no. 4 (2014): 250, doi: 10.1037/tam0000024.

[77] Borum et al., "Threat Assessment: Defining an Approach for Evaluating Risk for Targeted Violence," 333.

[78] Jarvis and Scherer, *Mass Victimization-Promising Avenues for Prevention*, 31.

[79] Ibid., 32.

[80] Ibid.

[81] Ibid.

[82] Ibid.

become violent and usually do not represent the violent stereotypes common in the public.[83]

An analysis of the Exceptional Case Study Project led Fein and Vossekuil to conclude that of those who had attempted assassination of public figures in the United States since 1949, mental illness only rarely played a role in assassination behaviors and the attackers functioned in deliberative and rational ways.[84] Since many people afflicted with mental illness are well organized, Borum et al. qualify the importance of mental illness by adding that it is best used as a measure of someone's functional ability to carry out an attack.[85] Hoffman, Meloy, and Sheridan confirm the functionality of the mentally ill upon their review of the literature. Their piece entitled "Contemporary Research on Stalking, Threatening, and Attacking Public Figures," and appearing in the *International Handbook of Threat Assessment*, states, "serious mental disorder does not mitigate the risk of a planful [sic] attack on a public figure. All studies indicate that despite the presence of mental illness, subjects can carefully plan an attack over the course of days, weeks, or months."[86]

6. Social Media and Threat Assessment

Understanding the influences of social media on group behavior and individual human nature allows for the opportunity to provide the context against which judgments may be made concerning threat assessments. Terror organizations, homegrown violent extremists, looming school shooters, and others considering violence, manifest themselves in unique ways via social media.

This influence presents the question of why social media is so effective for groups, such as ISIS or street gangs, prompting additional questions as to how it should

[83] Jarvis and Scherer, *Mass Victimization-Promising Avenues for Prevention*, 32.

[84] Fein and Vossekuil, *Protective Intelligence Threat Assessment Investigations*, 13.

[85] Borum et al., "Threat Assessment: Defining an Approach for Evaluating Risk for Targeted Violence," 333.

[86] Jens Hoffman, J. Reid Meloy, and Lorraine Sheridan, "Contemporary Research on Stalking, Threatening, and Attacking Public Figures," in *International Handbook of Threat Assessment*, ed. J. Reid Meloy and Jens Hoffmann (New York: Oxford University Press, 2014), 172.

be analyzed. The research on this offers something compelling as it pertains to jihadists. Although, this literature review explores more regarding social media than matters relative to radical Islam or jihadists' use of it. Writing in the journal, *Behavioral Sciences of Terrorism and Political Aggression,* researchers Sam Mullins and Adam Dolnik speculate on the nature of the "virtualization" of jihad and a subculture of "cool" that has grown around it.[87] Mullins and Dolnik assert that this subculture, combined with the rare presence in the West of an experienced mujahidin (Islamic warrior), increases dissociation from reality in the mind of the consumer of such propaganda and elevates the mythological value of the message.[88] Further, they noted the work of LTC (ret) Dave Grossman and his book entitled, *On Killing: The Psychological Cost of Learning to Kill in War and Society*, by adding "the impersonal, indiscriminate nature of terrorism is an ideal vehicle for fantasy, since psychologically it is easier to kill when removed from the victim."[89] These variables may help explain the attraction for disaffected youth who wish to use violence against an overbearing and dehumanized enemy.[90]

Social network analysis (SNA) is an avenue of research that offers promise when evaluating the manner in which Islamist terror cells may develop in the West, as well as the influence social media has on this process. Mullins and Dolnik explore the utility of SNA and identify several important considerations. First, they argue that group dynamics are important when considering contemporary Islamist terrorism in the West, as such terrorism is born from decentralized and evolving networks of people.[91] Further, they argue that group interaction is a powerful component to the elements of radicalization.[92] Published in November 2009, Mullins' and Dolnik's study could not have foreseen the growth in social media integration into U.S. society of 2015, nor the emergence of ISIS

[87] Sam Mullins and Adam Dolnik, "An Exploratory, Dynamic Application of Social Network Analysis for Modelling the Development of Islamist Terror-cells in the West," *Behavioral Sciences of Terrorism and Political Aggression* 2, no. 1 (January 2010): 15, doi: 10.1080/19434470903319441.

[88] Ibid.

[89] Ibid.

[90] Ibid.

[91] Ibid., 5.

[92] Ibid.

or other groups flourishing as a result of their social media success. Some relevance is lost since it was conducted, as it only considered group dynamics of Islamist terrors groups as predominately influenced by social settings, such as mosques, youth clubs, and gyms.[93] Social media was not considered at the time of publication. The authors did acknowledge the emerging influence of the internet by reporting that "more recently, operational terrorist groups have been described as increasingly self-reliant, utilizing the Internet both as a meeting point and as a source of ideological and operational information in the absence of formal organizational support or control," adding that the "'virtualization"' of jihad indicates that spontaneous interaction among groups has greater significance and potential to push people beyond radicalization to terrorist violence.[94] Notwithstanding the age of this piece of research, it more broadly dealt with SNA and its utility at understanding and disrupting people prior to violent action. It emphasized that it is important to understand group behavior and those that make up groups to understand better the relationships between behavior and social structure.[95]

The influence of social media presents an entirely new element to this conversation. Margarita Jaitner of Karlstad University in Sweden offers analysis that builds on the work of Mullins and Dolnik. Writing in 2014, Jaitner points out that social media represent an attack vector that must be considered by law enforcement.[96] Regarding groups and group behaviors as influenced by social media, she states, "unlike previously, many groups today consist of a large but very loosely connected network. This lack of cohesion can present a challenge for authorities, to identify emerging key actors and assess threat levels. Second, a high level of web penetration has allowed groups to ad-hoc organize, amend plans, and redirect physical activities."[97]

[93] Mullins and Dolnik, "An Exploratory, Dynamic Application of Social Network Analysis for Modelling the Development of Islamist Terror-cells in the West," 5.

[94] Ibid., 6.

[95] Ibid., 24.

[96] Margarita Jaitner, "Countering Threats: A Comprehensive Model for Utilization of Social Media for Security and Law Enforcement Authorities," *International Journal of Cyber Warfare and Terrorism* 4, no. 2 (April 2014): 35, doi: 10.4018/ijcwt.2014040103.

[97] Ibid.

7. Social Media Indicators and Social Identity Theory

Schmalz, Colistra, and Evans conducted research pertaining to social identity theory and the influences social media may have. Their study does not directly address gang and gang behavior, but it does emphasize important elements that dovetail with more specific research on this topic, which follows. This study approaches social identity theory and social media from a perspective unrelated to terrorism or active shooters, but it is relevant because it addresses validated principles associated with social identity theory and the manner in which social media has evolved to impact people's sense of self-worth and esteem. This viewpoint is applicable to the literature that follows concerning the manner by which threat assessments may be conducted via social media analysis.

Dorothy Schmalz, Craig Colistra, and Katherine Evans note that individuals striving to achieve high self-esteem may employ identity management strategies should their group be devalued.[98] They note that when a social group is devalued or marginalized, the social identity of an individual belonging to this group may likewise be diminished as a result.[99] Some compensate by taking action to reinforce their identities while others may conclude that group membership no longer serves them and withdraw.[100] This process may have implications for the analysis of social media activity and posts when considering whether or not one poses a threat to others.

8. Gangs and Violence—Opportunities for Threat Management

Examples of this phenomenon commonly occur throughout American cities in recent years, whereby urban youths associated with crime and street gangs are committing violence against one another stemming from offenses taken and given via social media.

[98] Dorothy Schmalz, Craig Colistra, and Katherine Evans, "Social Media Sites as a Means of Coping with a Threatened Social Identity," *Leisure Sciences* 37 (June 12, 2014): 22.

[99] Ibid.

[100] Ibid.

A 2015 *Los Angeles Times* article by Sandy Banks chronicled the evolution of gang violence and the influence of social media. The article quoted LAPD Deputy Chief Bob Green who stated, "Gangs are less hierarchical and more impulsive. They're not as likely to feud over turf or look to 'shot callers' for orders. And the spats that lead to shootings more often are linked to insults exchanged on social media than to the wrong color shoes or stare-downs at the park."[101] Later, Ms. Banks describes the frustration felt by law enforcement when threats are made via social media but become known to the police too late to have a preventive impact.[102] Consequently, the response has been to train and hire personnel who can look for trends or threats via social media to give the police a chance to disrupt potential violence, as the older techniques of community policing are proving to be less effective in this evolving environment.[103]

Highlighting the evolution of contemporary culture as influenced by social media, Desmond Patton, Robert Eschmann, and Dirk Butler presented a 2013 study into social media on the phenomenon of "internet banging." The authors assert that social media accounts are as important to gang members as guns.[104] Social media forums are used to trade insults with rivals, brag about crimes committed, and project threats that often result in real acts of violence, often murder.[105] The authors refer to concepts of collective identity and collective memory to help understand the power of social media on gang members and all human groups.[106] The authors contend that internet banging is the result of "the problematic urban masculine identity born out of a collective identity formulation that has been shaped over time by certain social, political, and economic forces throughout American history."[107] This assertion is akin to those of Schmalz when

[101] Sandy Banks, "'Cyber Banging' Drives New Generation of Gang Violence," *Los Angeles Times*, sec. Local/Crime & Courts, October 3, 2015, http://www.latimes.com/local/crime/la-me-1003-banks-lapd-gang-shootings-20151003-column.html.

[102] Ibid.

[103] Ibid.

[104] Desmond Upton Patton, Robert D. Eschmann, and Dirk A. Butler, "Internet Banging: New Trends in Social Media, Gang Violence, Masculinity and Hip Hop," *Computers in Human Behavior* 29, no. 5 (September 2013): A54, doi: 10.1016/j.chb.2012.12.035.

[105] Ibid.

[106] Ibid., A57.

[107] Ibid.

introducing social identity theory as a way to understand the weight of social media's influence upon groups and individuals. This understanding may contribute to new opportunities to identify people or groups who are developing intent and capability to commit violence.

The previously mentioned study by Jaitner makes recommendations concerning the manner in which proactive monitoring of social media should occur by authorities. She emphasizes the importance of establishing a framework by which social media should be considered.[108] Conveniently, Jaitner also ties this process to the evaluation of group activities or potential by recommending that when atypical social media is noted detected and analyzed, efforts should be made by law enforcement to disrupt potential violence or unrest that may occur.[109] The research previously noted contributes to an understanding of social media's power as a communication tool and its effectiveness with reaching and influencing others who may be on a pathway to violence.

9. Technological Aides to the Threat Assessor

It may be concluded from these examples that opportunities to detect leakage via social media should be abundantly available, perhaps too available to manage with available staff. This problem may be addressed through additional research into personnel training and assignments coupled with technological opportunities to help. Technology offers the concept of automated text analytics, which are processes by which software and other automated systems may process written material on the internet or social media and draw conclusions about it without human judgment or influence.

Referencing the need for additional resources to address the social media leakage problem, Cohen et al. note that opportunities exist for threat assessors and then delve into them. First, they describe text analysis techniques for analyzing social media.[110] Written in 2014, the authors describe these to be *translation services, sentiment analysis,*

[108] Jaitner, "Countering Threats," 43.

[109] Ibid.

[110] Cohen et al., "Detecting Linguistic Markers for Radical Violence in Social Media," 250.

mapping websites, and *author* recognition.[111] Each has promise. Translation services are often associated with free tools, such as those provided by Google that translate text for consumers.[112] This technology is frequently used in fusion centers and police departments through commercial vendors capable of social media observation that includes functionality for keyword searches and reverse translation services.

Sentiment analysis is described as the analysis of texts or mining methods of opinions appearing via social media and the internet.[113] Possibilities exist in this area to offset the large volume of open source social media traffic that may be vetted by a mechanized process and well-crafted computer algorithms.[114] Additionally, Bo Pang and Lillian Lee explored the advent of this concept and associated technology in a 2008 article entitled, "Opinion Mining and Sentiment Analysis," which appeared in the journal *Foundations and Trends in Information Retrieval*. Written to an audience interested in marketing and other business related enterprises, the article retains relevance to threat assessment as it speaks to common technologies and human behaviors observed when using them. Pang and Lee state, "aside from individuals, an additional audience for systems capable of automatically analyzing consumer sentiment, as expressed in no small part in online venues, are companies anxious to understand how their products and services are perceived."[115] The motivation of the companies mentioned in this quote likely extends to the police and security agencies in need of such technology for similar purposes. Security services will benefit from such technological developments made for the private sector by observing and assessing various forms of social media postings to glean threats and determine relevant courses of action. Incorporating automation into such a process may help reduce human oversights of potential leakage into social media postings.

[111] Cohen et al., "Detecting Linguistic Markers for Radical Violence in Social Media," 251.

[112] Ibid.

[113] Ibid.

[114] Ibid.

[115] Bo Pang and Lillian Lee, "Opinion Mining and Sentiment Analysis," *Foundations and Trends in Information Retrieval* 2, no. 1–2 (2008): 4, doi: 10.1561/1500000001.

Michal Kosinski, David Stillwell, and Thore Graepel note that through automation, basic digital records can be used to determine a host of individual characteristics that people would typically assume to be private.[116] Such a concept has implications for threat assessments, as it explores the opportunities to observe the difficulty in detecting leakage of hunters versus the less threatening but prolific verbiage of the howler. Their study dealt with information and conclusions able to be gleaned by analyzing the “like” feature of Facebook and the items that Facebook users acknowledged by clicking the “like” feature within Facebook. The study demonstrated that with analysis of the “like” feature, much may be determined about a particular Facebook user to include predictors of intelligence levels, male homosexuality, male heterosexuality, ethnicity, political views, and religious preferences.[117] Such studies offer a glimpse into the possibilities of technological options to assist with threat management.

The concept of a threat triage is further developed in Chapter 21 of the *International Handbook of Threat Assessment*. The authors, Sharon S. Smith, Robert B. Woyach, and Mary Ellen O’Toole look at the anonymous threatener and use the analogy of searching for a needle in a haystack.[118] The study addresses the use of language to predict approach and violence.[119] Identifying the factors that may serve as predictors of violence is important, as are processes for improving the accuracy of these predictors.[120] The study then introduces the Threat Triage, which is a web-based software tool to assess linguistic characteristics of threatening messages.[121] This software offers assessment of risk associated with a message as low, medium, or high and also calculates the probability that a message will be followed by targeted violence or approach behavior.[122]

[116] Michal Kosinski, David Stillwell, and Thore Graepel, “Private Traits and Attributes Are Predictable from Digital Records of Human Behavior,” *Proceedings of the National Academy of Sciences of the United States of America* 110, no. 15 (April 9, 2013): 5802.

[117] Ibid., 5805.

[118] Sharon S. Smith, Robert B. Woyach, and Mary Ellen O’Toole, “Threat Triage: Recognizing the Needle in the Haystack,” in *International Handbook of Threat Assessment*, ed. J. Reid Meloy and Jens Hoffmann (New York: Oxford University Press, 2014), 321.

[119] Ibid., 322.

[120] Ibid.

[121] Ibid., 323.

[122] Ibid.

The authors conclude the chapter by asking, "How do we discriminate between those who inappropriately communicate dramatic but empty rhetoric from those who communicate, then approach and harm?"[123] Whether using technology to analyze threats already made or using it to detect threats communicated through social media, a definite place for technological solutions exists to be used to help manage the threats coming to the attention of assessors, which allows for greater inspection of larger amounts of data and improved the accuracy with which the analysis is conducted.

Threat assessment is an inexact process made more challenging when inspecting social media commentary. Merging technological advancement and improved processes may contribute to greater accuracy and improvements when preventing violence from occurring.

10. Fusion Centers and the Violence Prevention Effort

Prevention of violence has taken on a new urgency in contemporary times and resources and techniques are being marshaled to improve the effectiveness of the overall effort. Academia, law enforcement, mental health providers, the private sector, and others are working together for this purpose. The American Psychological Association even released a new journal in 2014 dedicated to preventive threat assessment entitled the *Journal of Threat Assessment and Management*.[124]

Fusion centers arose en masse following the investigation into the causes of the terror attacks endured by the United States on September 11, 2001, known as 9/11. Building on the original terrorism mission, the all hazards-all crimes model of fusion centers has become the operational standard.[125] In other words, the scope of analytical

[123] Smith, Woyach, and O'Toole, "Threat Triage: Recognizing the Needle in the Haystack," 327.

[124] Anna Miller, "Threat Assessment in Action," *Monitor on Psychology* 45, no. 2 (February 2014): 37.

[125] United States Department of Justice, *Baseline Capabilities for State and Major Urban Area Fusion Centers* (Washington, DC: United States Department of Justice, September 2008), 24, http://it.ojp.gov/documents/d/baseline%20capabilities%20for%20state%20and%20major%20urban%20area%20fusion%20centers.pdf.

effort is broad and that fusion centers are expected to support the growing needs of local, state, and federal law enforcement in the United States.[126]

Part of the current effort to combat crime and terrorism is integration of the NSI-SAR.[127] Based upon identifiable and validated behaviors, this effort seeks to prevent crime and terrorism by using fusion centers to gather and share information pertaining to crime or terrorism patterns or trends.[128] State and local fusion centers serve as primary areas of focus for the collection, analysis, and sharing of suspicious activity reporting (SAR) information.[129]

Accustomed to collecting, analyzing, and sharing behavioral-based information, the processes and policies already in place by fusion centers may be leveraged to implement the behavioral-based methodology known as behavioral threat assessment. This implementation may increase opportunities to prevent mass or targeted violence in support of all crime missions. The prevention of violence, whether motivated by terrorism or some other cause, may be improved by enlisting the nation’s fusion centers through a convergence of policies pertaining to the collection of behavioral information, behavioral analysis, threat assessment, and coordinated threat management.

D. METHODOLOGY

Policy analysis is the methodology used for this study. This research evaluates policies currently in use by police agencies to prevent targeted violence and evaluates them for suitability of use by fusion centers to engage in the effort to prevent mass or targeted violence. Opportunities to modify policies already in use by fusion centers for this purpose are also explored.

[126] International Association of Chiefs of Police, *Razing Expectations-Erecting a Strategic Vision for Fusion Centers* (Alexandria, VA: International Association of Chiefs of Police, 2009), 1, http://www.theiacp.org/portals/0/pdfs/RazingExpectations.pdf.

[127] “Nationwide SAR Initiative (NSI)—About the NSI.”

[128] Nationwide SAR Initiative, *Information Sharing Environment Functional Standard SAR 1.5.5* (Washington, DC: Bureau of Justice Assistance, 2015), 9, https://nsi.ncirc.gov/documents/SAR_FS_1.5.5_PMISE.pdf.

[129] “Nationwide SAR Initiative (NSI)—About the NSI.”

III. THREATS AND VIOLENCE

A. INTENDED AND TARGETED VIOLENCE

Murderous violence takes many forms and those who engage in it do so for a host of reasons. However, the school shooters, lone actor terrorists, stalkers, political assassins, and even sadistic serial rapists and killers, engage in their crimes through deliberate and premeditated processes. These processes represent *intended violence* versus violence associated with crimes for profit or passion.[130] Intended violence differs from violence stemming from a profit motive or violence resulting from an emotional release (passion).[131] Thus, those who commit these types of violence engage in deliberate and elaborate planning processes including preparatory decisions or actions.[132]

Intended violence is unique in that a wide range of variables may cause it as opposed to a singular objective (such as financial gain).[133] Intended violence may stem from people motivated by an ideology, intent to act on delusions, efforts to acquire fame or notoriety, revenge, or killing classmates or coworkers.[134] Preventing crimes for profit or passion requires that the cost to a perpetrator be elevated to make the risk unacceptable or to defuse the emotion that drives someone to commit a passion-based crime.[135] However, prevention of intended violence requires more.

B. COUNTERMEASURES TO VIOLENCE—RESPONSE

Compared to crimes for profit or passion, intended violence is multi-faceted. Violence stemming from passion is spontaneous, not premeditated, and is often generated in the heat of the moment through emotional conflict.[136] By contrast, intended violence

[130] Calhoun and Weston, *Contemporary Threat Management*, 16.

[131] Ibid., 17.

[132] Fein, Vossekuil, and Holden, *Threat Assessment: An Approach to Prevent Targeted Violence*, 3.

[133] Calhoun and Weston, *Contemporary Threat Management*, 17.

[134] Ibid.

[135] Ibid., 16.

[136] Ibid.

includes intent coupled with plans to damage, injure, or kill someone without an uncontrollable passion or a motive for profit.[137] Disrupting intended violence requires the identification of a potential aggressor, assessment of the risk, and a strategy to manage a person away from violence.[138] This scenario presents challenges for those involved in public safety because people who may be progressing toward violence are hard to detect and disrupt. Thankfully, the processes of behavioral threat assessment and management have been developed and may help to help overcome these challenges.

Incidents of unforeseen violence present exceptional challenges to security services and the public. Examples include active shooters, stalkers of political figures or celebrities, workplace attackers, gang violence, terror attacks, and more.

Since 70% of active shooting incidents end in less than five minutes and 36% end in two minutes or less,[139] the public has been encouraged to consider its own counter-measures since a police response to an active shooter is often not fast enough to prevent the loss of life. The FBI notes a publicly released 2013 video created by the Houston Mayor's Office of Public Safety and Homeland Security entitled "Run. Hide. Fight. Surviving an Active Shooter Incident"[140] that provides guidance to citizens regarding ways to protect themselves and others during an active shooting incident. The video portrays a fictional active shooting incident in an urban setting and the reactions of those affected.[141] It illustrates the vulnerability of people when faced with an active shooter.

Concluding its 2013 analysis of active shooter incidents between 2000 and 2013, the FBI reported that the avoidance of active shooter tragedies is most desired, emphasizing the importance of prevention efforts.[142] Writing in the *Small Wars Journal*, Ryan Hoover and Daniel Shaw emphasize the importance of preparation for active

[137] Calhoun and Weston, *Contemporary Threat Management*, 16.

[138] Ibid., 17.

[139] Blair and Schweit, "A Study of Active Shooter Incidents, 2000–2013," 8.

[140] "Run. Hide. Fight. Surviving an Active Shooter Event."

[141] Ibid.

[142] Blair and Schweit, "A Study of Active Shooter Incidents, 2000–2013," 21.

shooter incidents.[143] The authors note that many victims of active shooters fail to fight back or otherwise subdue an attacker due to a lack of basic skills and awareness of how to act during such situations.[144] The merits of running, hiding, or fighting are typically considered with hindsight, after a shooting event has occurred. Hence, attention is given to techniques and methods for potential victims to defend themselves once an active shooting has begun. These recommendations do not include assistance from law enforcement because it is assumed that an adequate law enforcement response cannot happen fast enough to make a difference. Essentially, those targeted by active shooters are on their own and against long odds, must make fast and desperate decisions when attempting to survive.

Running, hiding, and fighting are last resort tactics to employ when faced with an active shooter event. While important to know, it is also important to consider opportunities to prevent mass shootings when possible. Behavioral threat assessment and management offers the opportunities to prevent mass or targeted attacks.

C. COUNTERMEASURES TO VIOLENCE—PREVENTION

Considering this reality, for law enforcement to be of service, prevention is recommended as the most likely strategy for success. As mass victimization events are rare, a persistent notion pervades that “it won’t happen here;” thus leading to a lack of preparation.[145] Behavioral threat assessment is an important element of the preventive effort.[146] The literature concerning active shooting incidents and other forms of mass or targeted violence reveals techniques by which assessments of potentially violent behavior may be accomplished. It also offers hope for prevention and encourages the awareness that tragedies, such as mass shootings, are not inevitable or unstoppable; they can be prevented.[147]

[143] Ryan Hoover and Daniel Shaw, “How to Stop an Active Killer,” *Small Wars Journal*, June 29, 2016, 1.

[144] Hoover and Shaw, “How to Stop an Active Killer,” 2.

[145] Jarvis and Scherer, *Mass Victimization-Promising Avenues for Prevention*, 7.

[146] Ibid.

[147] Miller, “Threat Assessment in Action,” 1.

Currently, research is evolving and growing as it pertains to violent incidents, indicators of pending violence, threat assessment protocols, and techniques by which to study or prevent violence. Threats of violence are diverse. However, opportunities to detect and possibly prevent violent acts exist in the rapidly evolving world of social media.

D. TERRORIST THREATS AND SOCIAL MEDIA—EVOLUTION AND UTILIZATION

Social media, alternatively known as Web 2.0, is a quickly evolving means of communication, with ramifications for disciplines, such as law enforcement and homeland security. Today, social media is regarded as being a significant recruiting tool used by foreign terror organizations, such as Islamic State in Iraq and Syria (ISIS). Examples are available whereby ISIS uses social media to identify and recruit like-minded people to its cause by posting images of graphic and sensational violence, such as shootings, beheadings, and other elements of jihad meant to be alluring to the viewer. Pertaining to social media engagement and its usefulness to recruit, ISIS members have remarked, “don’t hear about us, hear from us.”[148] This remark represents a strategic adjustment by ISIS to assert control over the way its messages are received instead of allowing the mass media to control the narrative, as had been done in the past with its rival Al Qaeda.[149]

Michael Weiss and Hassan Hassan, in their book entitled *ISIS—Inside the Army of Terror*, observe that the terror organization has adapted to messaging problems that hindered earlier jihadi groups and is instead using social media to combat this problem.[150] They go on to point out that social media services, such as Twitter and Facebook, are effective and allow for large-scale messaging or crowd sourcing in spontaneous fashion.[151] As an example, ISIS has been successful with its effort to cause

[148] Michael Weiss and Hassan Hassan, *ISIS—Inside the Army of Terror* (New York: Regan Arts, 2015), 171.

[149] Ibid., 170.

[150] Ibid., 171.

[151] Ibid., 170.

people to hear from it directly by creating pseudo-documentaries containing sermons coupled with violent theology and imagery.[152] Oddly, these propaganda and recruitment productions feature content that many Western politicians and diplomats have felt would diminish people's attraction to such groups.[153] While containing graphic and horrifying images, the productions have been attractive to those new to ISIS and not repulsive.

This attraction presents the question of why social media is as effective as it pertains to groups, such as ISIS, and offers further questions as to how it should be mitigated. The research on this topic offers something compelling as it pertains to jihadists. A "virtualization" of jihad and a subculture of "cool" has grown around it.[154] Lieutenant Colonel (ret) Dave Grossman, in his book entitled, *On Killing: The Psychological Cost of Learning to Kill in War and Society*, stated, "the impersonal, indiscriminate nature of terrorism is an ideal vehicle for fantasy, since psychologically it is easier to kill when removed from the victim."[155] These variables may help explain the attraction for disaffected youth who wish to use violence against an overbearing and dehumanized enemy. The influence of social media presents an entirely new attack vector that must be considered by law enforcement.[156]

[152] Weiss and Hassan, *ISIS—Inside the Army of Terror*, 171.

[153] Ibid.

[154] Mullins and Dolnik, "An Exploratory, Dynamic Application of Social Network Analysis for Modeling the Development of Islamist Terror-cells in the West," 15.

[155] Dave Grossman, *On Killing: The Psychological Cost of Learning to Kill in War and Society* (New York: Integrated Media Incorporated, 2014), Kindle location 2618, Kindle edition.

[156] Jaitner, "Countering Threats," 35.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. THE EVOLUTION AND INFLUENCE OF FUSION CENTERS

A. HISTORICAL CONTEXT

Historically, police departments in the United States have been reactive by responding to calls for service and investigating crimes and preparing cases for criminal prosecution.[157] However, school shootings, assassinations, terrorist attacks, and other instances of mass or targeted violence necessitates that law enforcement agencies identify effective strategies to prevent these problems. As with other types of crimes, the traditional role of law enforcement in mass victimization incidents has been reactive, as demonstrated through the evolution of the tactical response protocols to such incidents.[158] While the tactical changes were necessary, it is now recognized that efforts to prevent mass casualty incidents are worthy of pursuit.[159] Prevention is challenging. It must be accomplished while respecting and preserving civil rights, civil liberties, and the privacy of those who come under scrutiny for the potential to commit violence, as well as their potential victims. Organized police forces in the United States began by adopting the preventive patrol model first established in the United Kingdom in 1829 with the creation of the London Metropolitan Police.[160] Prevention, in this context, was promoted through the patrols of uniformed police officers with the hope of altering criminal inclinations of people due to an overt police presence, thereby preserving public order.[161] As American policing evolved, it was discovered that the early strategies of random patrols and answering calls for service were not resulting in significant reductions in crime rates.[162] Consequently, community-policing strategies were born.[163] Generally, these efforts focus on utilizing the police to improve the quality of life in neighborhoods

[157] Fein, Vossekuil, and Holden, *Threat Assessment: An Approach to Prevent Targeted Violence*, 2.

[158] Jarvis and Scherer, *Mass Victimization-Promising Avenues for Prevention*, 4.

[159] Ibid.

[160] Craig D. Uchida, "The Development of the American Police," *Critical Issues in Policing: Contemporary Readings*, December 2004, 8.

[161] Ibid., 11.

[162] Ibid., 28.

[163] Ibid.

by developing strong community ties to craft tailored solutions to localized problems.[164] The development of these strategies may serve the homeland security enterprise as quickly as the local neighborhood watches because the smallest of details, if reported to the right person or agency, may be the decisive variable in whether or not an act of mass violence is prevented.

Fusion centers serve as the intersections between the public, private industry, police officers at each level of government, fire fighters, mental health providers, public health providers, and other public safety stakeholders. These junctions may be a good place to combine the totality of details in possession of each stakeholder for the purpose of analyzing certain situations or circumstances to help prevent violence.

A 2012 article in *Police Chief Magazine* illustrates this junction and highlights its value. The author of the article is Lieutenant Colonel Ray Guidetti of the New Jersey State Police. Guidetti notes several examples whereby the New Jersey Regional Operations Intelligence Center (NJ ROIC) successfully supported local police agencies by providing intelligence and crime analysis to improve resource deployment, support cold case investigations, gun crime analysis, leverage state resources to help resolve local problems, and real-time tactical investigations, such as multi-agency responses to homicides.[165] Overall, Guidetti persuasively makes the case that fusion centers, such as the ROIC in New Jersey, have much to offer local police departments beyond traditional terrorism analysis. Like many fusion centers, the ROIC is made up of personnel from a host of federal, state, and local agencies and is co-located with the New Jersey Office of Emergency Management.[166] Guidetti notes that fusion centers, such as the ROIC, are "gateways" to the federal government on behalf of localities by providing access to the intelligence community (the FBI and the Department of Homeland Security (DHS)) through SAR that begins at the local level.[167]

[164] Uchida, "The Development of the American Police," 29.

[165] Ray Guidetti, "Local Policing: Expanding Reach with Limited Resources through Fusion Centers," *The Police Chief*, February 2012, 22.

[166] Guidetti, "Local Policing: Expanding Reach with Limited Resources through Fusion Centers."

[167] Ibid.

B. NATIONAL NETWORK

Since 9/11, international terrorism and large-scale attacks by foreign terrorist organizations led to a change in mission focus by federal law enforcement and intelligence agencies. This new focus was directed at foreign terrorist organizations, most notably Al Qaida.[168] Also following 9/11, numerous state and local agencies across the country worked to support this effort through the establishment of fusion centers in their areas of responsibility.[169]

As the number of fusion centers has steadily grown from a handful in the early years following the terror attacks of 9/11 to 78 today, each is under the control of a state or local authority.[170] Being a decentralized network, the focus of each center is unique.[171] The National Network of Fusion Centers is a collaborative network of independent fusion centers designed to support and advance the capabilities and value of each center and the network as a whole.[172] Organized as state or local entities with varying designs, the fusion centers of the network have evolved over time from a terrorism focus to today's more common all-hazards, all-crimes models. This evolution has been criticized as mission creep by some observers who posit that international terrorism should remain the exclusive focus of fusion center efforts.[173] Nevertheless, the

[168] David Brannan, Kristin Darken, and Anders Strindberg, *A Practitioner's Way Forward* (Salinas, CA: Agile Press, 2014), 74.

[169] National Fusion Center Association, *National Strategy for the National Network of Fusion Centers*, 2014, 1, https://nfcausa.org/html/National%20Strategy%20for%20the%20National%20Network%20of%20Fusion%20Centers.pdf.

[170] Erik Dahl, "Domestic Intelligence Today: More Security but Less Liberty?," *Homeland Security Affairs* 7, no. 2 (2011): 5, http://search.proquest.com/openview/710cc09449b7b0d18bd97395ee5ad261/1?pq-origsite=gscholar.

[171] Ibid.

[172] National Fusion Center Association, *National Strategy for the National Network of Fusion Centers*, 9.

[173] Torin Monahan and Neal A. Palmer, "The Emerging Politics of DHS Fusion Centers," *Security Dialogue* 40, no. 6 (December 1, 2009): 626, doi: 10.1177/0967010609350314.

Fusion Center Guidelines recommends the all-hazards-all crimes approach to operating fusion centers.[174]

Since the FBI reorganized its mission in the early 2000s to prioritize terrorism and domestic intelligence collection to address the terrorism threat to the nation, the mission space for fusion centers to address international terrorism issues is largely occupied.[175] However, information sharing among partners remains the core responsibility of fusion centers; thus, the emphasis upon terrorism remains a priority.[176]

As fusion centers matured, their analytical capabilities began to be leveraged for priorities beyond international terrorism.[177] The all-hazards-all crimes model emerged for fusion centers after being recommended as part of the 2004 *Final Report of the Homeland Security Advisory Council's Intelligence and Information Sharing Initiative*.[178] All hazards intelligence has been equated to homeland security intelligence and is defined as "the collection and analysis of information concerned with noncriminal domestic threats to critical infrastructure, community health, and public safety for the purpose of preventing the threat or mitigating the effects of a threat."[179]

Public safety representatives from federal, state, and local law enforcement, the fire service, emergency management, corrections, public health, the National Guard, and a host of other federal, state, and local agencies combine in various ways to form the

[174] Criminal Intelligence Coordinating Council, *Fusion Center Guidelines: Law Enforcement Intelligence, Public Safety, and the Private Sector* (Washington, DC: Criminal Intelligence Coordinating Council, 2006), 10, https://it.ojp.gov/gist/94/Fusion-Center-Guidelines--Law-Enforcement-Intelligence--Public-Safety--and-the-Private-Sector.

[175] David L. Carter, *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies*, 2nd ed. (Washington, DC: U.S. Department of Justice Office of Community Oriented Policing Services, January 2009), 38, https://it.ojp.gov/documents/d/e050919201-IntelGuide_web.pdf.

[176] National Fusion Center Association, *National Strategy for the National Network of Fusion Centers*, 8.

[177] Monahan and Palmer, "The Emerging Politics of DHS Fusion Centers," 626.

[178] Homeland Security Advisory Council, *Homeland Security Advisory Council Intelligence and Information Sharing Initiative—Final Report* (Washington, DC: U.S. Department of Homeland Security, 2004), 43.

[179] Carter, *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies*, 14.

nation's fusion centers. Coordination of these diverse agencies fits the all-hazards all-crimes approach to fusion center design and operation.[180]

As part of the all-hazards-all crimes approach, fusion centers may categorize analytical priorities by areas of specialty. Examples of these specialties may include terrorism, gangs, cyber security, critical infrastructure protection, public health, fire programs, general crimes, and others.[181] The analytical priorities of fusion centers are determined upon formal or informal processes by agency leadership or management.[182]

C. THE NATIONWIDE SUSPICIOUS ACTIVITY REPORTING INITIATIVE AND BEHAVIOR-BASED ASSESSMENTS

Receiving, analyzing, and processing reports of suspicious activities are a fundamental mission of fusion centers.[183] These reports help connect localized information to all levels of public safety depending on the nature and context of the information. These processes were identified as core capabilities that all fusion centers should address.[184] The NSI was developed to provide guidance on how fusion centers should triage reports of suspicious behavior they receive.[185] Raw perceptions made by untrained observers may be subjective; leading to spontaneous conclusions that something or someone is suspicious. Therefore, the NSI was created to vet suspicious activity reports and provide a mechanism by which privacy, civil rights, and civil liberties may be protected. This program identified seven validated behaviors associated with potential terrorism.[186]

[180] Criminal Intelligence Coordinating Council, *Fusion Center Guidelines*, 3.

[181] Monahan and Palmer, "The Emerging Politics of DHS Fusion Centers," 625.

[182] United States Department of Justice, *Baseline Capabilities for State and Major Urban Area Fusion Centers*, 7.

[183] Ibid., 13.

[184] Ibid.

[185] "Nationwide SAR Initiative (NSI)—About the NSI."

[186] Jeff Gruenewald et al., *Validation of the Nationwide Suspicious Activity Reporting (SAR) Initiative: Identifying Suspicious Activities from the Extremist Database (ECDB) and the American Terrorism Study (ATS),* Report to the U.S. Department of Homeland Security (College Park, MD: National Consortium for the Study of Terrorism and Responses to Terrorism (START), 2015), 12.

Fusion centers have adapted to making judgments about behaviors as part of the NSI. Fusion centers also support federal, state, and local police agencies by answering requests for information from their databases. Databases may include employment records, firearms transaction records, police records management data, and other information. The relationships between fusion centers and police departments are long-standing and have contributed to the evolution of the all-crimes all-hazards mission described previously.

The NSI Concept of Operations was created in 2008 to create a process by which behavioral information and incidents associated with crime could be shared in a structured way to help detect and prevent terrorism.[187] Therefore, an approach to considering suspicious activity grounded in behavioral observations allows for the elimination of useless criteria, such as race, ethnicity, gender, national origin, religion, sexual orientation, or gender identity as traits that may be used to validate suspicion.[188] As part of the NSI, 16 pre-operational behaviors have been identified to be reasonably indicative of terrorism and are shown in Table 1.[189]

Table 1. Defined Criminal Activity and Potential Terrorism Nexus Activity.[190]

Behavior	**Description**
Breach/Attempted Intrusion	Unauthorized personnel attempting to enter or actually entering a restricted area, secured protected site, or nonpublic area. Impersonation of authorized personnel (e.g., police/security officers, janitor, or other personnel).
Misrepresentation	Presenting false information or misusing insignia, documents, and/or identification

[187] U.S. Department of Homeland Security, *Nationwide Suspicious Activity Reporting Initiative Concept of Operations* (Washington, DC: U.S. Department of Homeland Security, 2008), 7, https://www.ise.gov/sites/default/files/NSI_CONOPS_Version_1_FINAL_2008-12-11_r1.0.pdf.

[188] Nationwide SAR Initiative, *Information Sharing Environment Functional Standard SAR 1.5.5,* 10.

[189] Ibid.

[190] Adapted from Nationwide SAR Initiative, S*uspicious Activity Reporting Indicators and Examples* (Washington, DC: Nationwide SAR Initiative, 2015), 3–4.

Behavior	Description
	to misrepresent one's affiliation as a means of concealing possible illegal activity.
Theft/Loss/Diversion	Stealing or diverting something associated with a facility/infrastructure or secured protected site (e.g., badges, uniforms, identification, emergency vehicles, technology, or documents {classified or unclassified}), which are proprietary to the facility/infrastructure or secured protected site.
Sabotage/Tempering/Vandalism	Damaging, manipulating, defacing, or destroying part of a facility/infrastructure or secured protected site.
Cyberattack	Compromising or attempting to compromise or disrupt an organization's information technology infrastructure.
Expressed or Implied Threat	Communicating a spoken or written threat to commit a crime that will result in death or bodily injury to another person or persons or to damage or compromise a facility/infrastructure or secured protected site.
Aviation Activity	Learning to operate, or operating an aircraft, or interfering with the operation of an aircraft in a manner that poses a threat of harm to people or property and that would arouse suspicion of terrorism or other criminality in a reasonable person. Such activity may or may not be a violation of Federal Aviation Regulations.

Table 2 shows the behaviors associated with the Nationwide SAR Initiative that may be indicative of criminal behavior or may be innocent. Context is required to evaluate these behaviors properly; thus, additional information is required before making conclusions or taking actions.

Table 2. Potential Criminal or Non-criminal Activity Requiring Additional Information During Vetting.[191]

Behavior	**Description**
Eliciting Information	Questioning individuals or otherwise soliciting information at a level beyond mere curiosity about a public or private event or particular facets of a facility's or building's purpose, operations, security procedures, etc., in a manner that would arouse suspicion of terrorism or other criminality in a reasonable person.
Testing or Probing of Security	Deliberate interactions with, or challenges to, installations, personnel, or systems that reveal physical, personnel, or cybersecurity capabilities in a manner that would arouse suspicion of terrorism or other criminality in a reasonable person.
Recruiting/Financing	Providing direct financial support to operations teams and contacts or building operations teams and contacts; compiling personnel data, banking data, or travel data in a manner that would arouse suspicion of terrorism or other criminality in a reasonable person.
Photography	Taking pictures or video of persons, facilities, buildings, or infrastructure in an unusual or surreptitious manner that would arouse suspicion of terrorism or other criminality in a reasonable person. Examples include taking pictures or video of infrequently used access points, the superstructure of a bridge, personnel performing security functions (e.g., patrols, badge/vehicle checking), security related equipment (e.g., perimeter fencing, security cameras), etc.
Observation/Surveillance	Demonstrating unusual or prolonged interest in facilities, buildings, or

[191] Adapted from Nationwide SAR Initiative, S*uspicious Activity Reporting Indicators and Examples*, 1–2.

Behavior	Description
	infrastructure beyond mere casual (e.g., tourists) or professional (e.g., engineers) interest and in a manner that would arouse suspicion of terrorism or other criminality in a reasonable person. Examples include observation through binoculars, taking notes, attempting to mark off or measure distances, etc.
Materials Acquisition/Storage	Acquisition and/or storage of unusual quantities of materials such as cell phones, pagers, radio control toy servos or controllers; fuel, chemicals, or toxic materials; and timers or other triggering devices, in a manner that would arouse suspicion of terrorism or other criminality in a reasonable person.
Acquisition of Expertise	Attempts to obtain or conduct training or otherwise obtain knowledge or skills in security concepts, military weapons or tactics, or other unusual capabilities in a manner that would arouse suspicion of terrorism or other criminality in a reasonable person.
Weapons Collection/Discovery	Collection or discovery of unusual amounts or types of weapons, including explosives, chemicals, and other destructive materials, or evidence, detonations or other residue, wounds, or chemical burns, that would arouse suspicion of terrorism or other criminality in a reasonable person.
Sector-Specific Incident	Actions associated with a characteristic of unique concern to specific sectors (e.g., the public health sector), with regard to their personnel, facilities, systems, or functions in a manner that would arouse suspicion of terrorism or other criminality in a reasonable person.

D. BEHAVIORAL THREAT MANAGEMENT—BEYOND THE NSI-TYPOLOGY OF WARNING BEHAVIORS

The aforementioned behaviors associated with the Nationwide SAR Initiative have been analyzed and scientifically validated by the National Consortium for the Study of Terrorism and Responses to Terrorism (START) at the University of Maryland.[192] This study utilized data taken from the *U.S. Extremist Database* and the *American Terrorism Study,* each of which contained data regarding U.S.-based terrorists and violent extremists and their activities and behaviors prior to the acts of violence they committed.[193] Researchers concluded that the pre-incident behaviors documented in the data align with the behavioral indicators of the Nationwide SAR Initiative.[194]

Similar to the Nationwide SAR Initiative and the behavioral indicators of interest, threat assessment practitioners also observe and document behaviors and behavioral patterns. Also like the Nationwide SAR Initiative, certain behaviors have been identified in the literature known as *warning behaviors,* indicative of observable behavioral changes that serve as evidence of a growing risk for violence and an increasing threat.[195] These behaviors are observable assuming that the ability to collect them exists via intelligence gathering operations.[196] Warning behaviors, as shown in Table 3, are defined and categorized, providing a comprehensive typology that serves those conducting assessments and developing management strategies.[197]

[192] Gruenewald et al., *Validation of the Nationwide Suspicious Activity Reporting (SAR) Initiative: Identifying Suspicious Activities from the Extremist Database (ECDB) and the American Terrorism Study (ATS)*, 14.

[193] Gruenewald et al., *Validation of the Nationwide Suspicious Activity Reporting (SAR) Initiative: Identifying Suspicious Activities from the Extremist Database (ECDB) and the American Terrorism Study (ATS)*, 1.

[194] Ibid., 14.

[195] J. Reid Meloy et al., “The Role of Warning Behaviors in Threat Assessment: An Exploration and Suggested Typology: Warning Behaviors in Threat Assessment,” *Behavioral Sciences & the Law* 30, no. 3 (May 2012): 260, doi: 10.1002/bsl.999.

[196] Ibid.

[197] Ibid.

Table 3. Typology of Warning Behaviors

Behavior	Description
Pathway Warning Behavior	Any behavior that is part of research, planning, preparation, or implementation of an attack.[198]
Fixation Warning Behavior	Any behavior that indicates an increasingly pathological preoccupation with a person or a cause.[199]
Identification Warning Behavior	Behavior that indicates a desire to be a "pseudo-commando,"[200] have a warrior mentality,[201] closely associate with weapons or other law enforcement paraphernalia, identify with attackers or assassins, or identify oneself as an agent to advance a particular cause or belief system.[202]
Novel Aggression Warning Behavior	An act of violence that appears unrelated to any targeted pathway warning behavior that is committed for the first time.[203]
Energy Burst Warning Behavior	An increase in the frequency or variety of any noted activities related to the target, even if the activities themselves are relatively innocuous, usually in the days or weeks before the attack.[204]
Leakage Warning Behavior	The communication to a third party of an intent to do harm to a target through an attack.[205]

[198] Calhoun and Weston, *Contemporary Threat Management*, 57.

[199] Paul E. Mullen et al., "The Fixated and the Pursuit of Public Figures," *Journal of Forensic Psychiatry & Psychology* 20, no. 1 (February 2009): 3, doi: 10.1080/14789940802197074.

[200] Park E. Dietz, "Mass, Serial and Sensational Homicides," *Bulletin of the New York Academy of Medicine* 62, no. 5 (1986): 482.

[201] J. Reid Meloy et al., "Offender and Offense Characteristics of a Nonrandom Sample of Adolescent Mass Murderers," *Journal of the American Academy of Child & Adolescent Psychiatry* 40, no. 6 (June 2001): 721, doi: 10.1097/00004583-200106000-00018.

[202] Meloy et al., "The Role of Warning Behaviors in Threat Assessment," 264.

[203] Ibid.

[204] Candice L. Odgers et al., "Capturing the Ebb and Flow of Psychiatric Symptoms with Dynamical Systems Models," *American Journal of Psychiatry* 166, no. 5 (May 2009): 580, http://ajp.psychiatryonline.org/doi/abs/10.1176/appi.ajp.2008.08091398.

[205] Meloy and O'Toole, "The Concept of Leakage in Threat Assessment," 514.

Behavior	Description
Last Resort Warning Behavior	Evidence of violent “action imperative.”[206] increasing desperation or distress through declaration in word or deed, forcing the individual into a position of last resort.[207] There is no alternative other than violence, and the consequences are justified.[208]
Directly Communicated Threat Warning Behavior	The communication of a direct threat to the target or law enforcement beforehand.[209] A threat is written or oral communication that implicitly or explicitly states a wish or intent to damage, injure, or kill the target, or individuals symbolically or actually associated with the target.[210]

[206] Kris Mohandie and James E. Duffy, “Understanding Subjects With Paranoid Schizophrenia,” *FBI Law Enforcement Bulletin* 68, no. 12 (1999): 12.

[207] Meloy et al., “The Role of Warning Behaviors in Threat Assessment,” 265.

[208] Gavin De Becker, *The Gift of Fear* (New York: Dell Publishing, 1997), Kindle location 1622, Kindle edition.

[209] Meloy et al., “The Role of Warning Behaviors in Threat Assessment,” 266.

[210] Meloy et al., “The Role of Warning Behaviors in Threat Assessment,” 266.

V. EXAMPLES OF BEHAVIORAL THREAT MANAGEMENT PROGRAMS

A. LAW ENFORCEMENT THREAT MANAGEMENT PROGRAMS

The notion of a "gateway" to the federal government, first described by LTC Guidetti, may apply more broadly whereby fusion centers may add value to this nation's security by offering behavioral threat assessments and behavioral threat management strategies for stakeholders at each level of government. Fusion centers may serve as gateways to each level of government by offering theses services.

Threat assessment and management has been studied in a variety of contexts and the literature offers options to establish threat assessment and management programs. Behavioral threat management is a process used to help prevent and mitigate violence through a proactive analysis of ideas and behaviors.[211] Those working to conduct behavioral threat assessment and management become aware of potential attackers by detecting them or receiving reports from others, assess the risk for violence, and craft strategies to prevent violence by managing the person or circumstances.[212] Today, police agencies are faced with the challenges of identifying and responding to threats of targeted violence before they occur while doing so in ways that avoid encroachment upon civil liberties.[213]

It is argued in this paper that fusion centers have a role in helping the arena of behavioral threat assessors and managers. This is consistent with and an extension of the all-hazards, all-crimes models of fusion centers that have evolved since fusion centers first began to appear nationally after 9/11. Also contributing to the need for fusion center engagement is the impact of social media as a growing dimension of communication among the public.[214] Some fusion centers are already observing and analyzing open

[211] Borum et al., "Threat Assessment: Defining an Approach for Evaluating Risk for Targeted Violence," 327.

[212] Fein, Vossekuil, and Holden, *Threat Assessment: An Approach to Prevent Targeted Violence*, 3.

[213] Harris and Lurigio, "Threat Assessment and Law Enforcement Practice," 52.

[214] National Fusion Center Association, *National Strategy for the National Network of Fusion Centers*, 7.

source materials through social media by utilizing tools for the purpose of maximizing situational awareness pertaining to a host of topics. Among these materials may include social media postings pertaining to civil unrest, threats against police officers, threats against political figures, threats against schools, threats to commit suicide, and others. Consequently, threats made via social media and the need to resolve them has led to a growing awareness. Certainly, open source analysis of social media may allow ample opportunities to detect *leakage* warning behavior, among others. Threats are also communicated in traditional ways, such as by telephone, postal mail, or interpersonal exchanges. Agencies partnering with fusion centers, such as police departments, correctional facilities, public health departments, and the general public, also report and share information.

Involvement of fusion centers in the process of threat management may create a new dimension to the traditional threat assessment programs already in existence with federal, state, and local police agencies in the United States or with the nation's campus threat assessment teams. As noted earlier, some fusion centers are engaged in the active observation and analysis of open-source social media for analytical and tactical purposes. Pursuit of this information may allow fusion centers to serve as force multipliers for traditional threat management programs or teams.

Police departments have developed threat management units in response to specific incidents, and fusion centers have been tailored to serve specific stakeholders who are mostly state or local sponsors.[215] However, the need to manage threats goes to the core function of fusion centers.[216] Beyond traditional SAR associated with counter-terrorism efforts, fusion centers with all-crimes-all hazards obligations must consider and evaluate other types of threats, such as those directed against public officials or celebrities, threats presented by stalkers, threats presented by intimate partners, or threats of mass shootings at schools or public gathering places.[217]

[215] National Fusion Center Association, *National Strategy for the National Network of Fusion Centers*, 2.

[216] Ibid., 7.

[217] Ibid., 9.

1. United States Secret Service

The USSS has a robust threat management program and is considered an originator of the process by which threats are detected and managed for the purpose of preventing acts of targeted violence against the President of the United States and other protectees.[218] The Secret Service's threat assessment approach is tailored to assessing and mitigating threats to those under its protection.[219] However, the threat assessment model used by the USSS is also applicable to the evaluation of violence risk for threats outside the scope of executive dignitary protection.[220]

The Secret Service's brand of threat assessment was born from an analysis of a study entitled the Exceptional Case Study Project (ECSP).[221] Lasting five years, the Secret Service partnered with the National Institute of Justice and the Federal Bureau of Prisons to study the thinking and behavior of those who, since 1949, were known to have attacked, or approached with intent to attack, American political figures or others with an elevated public profile.[222]

The ECSP results helped craft USSS threat assessment protocols but were also determined to be of value to those at every level of government with law enforcement and protective intelligence responsibilities.[223] Indeed, planned and targeted attacks affect many others beyond political figures or celebrities.[224] Prevention of violence is the primary objective and understanding the processes by which threats and vulnerabilities are gauged may offer real opportunities to disrupt deadly situations of mass or targeted violence successfully.[225]

[218] Borum et al., "Threat Assessment: Defining an Approach for Evaluating Risk for Targeted Violence," 323.

[219] Fein and Vossekuil, *Protective Intelligence Threat Assessment Investigations*, 14.

[220] Borum et al., "Threat Assessment: Defining an Approach for Evaluating Risk for Targeted Violence," 327.

[221] Fein and Vossekuil, *Protective Intelligence Threat Assessment Investigations*, 3.

[222] Ibid.

[223] Ibid.

[224] Ibid., 4.

[225] Ibid., 7.

Following the ECSP, the USSS documented the results and made a number of recommendations for federal, state, and local law enforcement personnel who may use threat assessment techniques as part of their protective security assignments. Among these recommendations are guidance points to establish and implement protective intelligence programs by asking some important questions.[226] These points include definitions of problems at hand, an identification of the scope and concept of a threat assessment program, an establishment of objectives, and an assessment of capabilities to make implementation possible.[227]

The concept of protective intelligence involves programs and systems used to identify someone who poses a threat and the proactive prevention of violence.[228] Also credited to the USSS, protective intelligence efforts are programs, whereby threat assessments are conducted and threat management strategies are devised as a result.

2. United States Marshals Service

Differing somewhat from the Secret Service's protective mission, the USMS is required by federal law to protect the federal judiciary.[229] Included are about 2000 federal judges, as well as the many U.S. attorneys and their assistants and staff.[230] Due to the vast number of protectees under its charge, the USMS must employee an analytical process by which threats are assessed and mitigated.[231]

Threat analysis within the USMS consists of three steps.[232] These steps include the initial reporting of suspicious circumstances to the USMS, analysis of the issue, and reporting of analytical results.[233] The USMS utilizes analysts to evaluate threats and

[226] Fein and Vossekuil, *Protective Intelligence Threat Assessment Investigations*, 23.

[227] Ibid.

[228] Ibid., 24.

[229] Debra M. Jenkins, "The U.S. Marshals Service's Threat Analysis Program for the Protection of the Federal Judiciary," *The Annals of the American Academy of Political and Social Science* 576, no. 1 (2001): 70.

[230] Ibid.

[231] Ibid.

[232] Ibid., 70.

[233] Ibid., 70–72.

communicate their conclusions to the USMS threat investigators for continued evaluation and follow-up.[234]

Threats or issues of concern that come to the attention of the USMS are often communications protected by the First Amendment of the United States Constitution.[235] Analysis is conducted to determine whether or not such communications meet the USMS definition of Inappropriate Communications or Contacts (IC&Cs).[236] The USMS defines IC&Cs as:

- "Assault or attempted assault on a judicial official.
- Suspicious Activity around a judicial official such as surveillance, vandalism or property damage, unusual activities at official's residence, or suspicious inquiries.
- Communication containing any single one of the following references, which are considered inappropriate:
    - Any threats, whether direct or specific, veiled ("You'll get yours"), or conditional ("You'd better do… or I will").
    - An extraordinary complaint or sense of outrage over the handling of a court case.
    - Pseudo-legal court filings from quasi-courts other than duly constituted federal, state, or local governments.
    - References to a special history or special destiny shared with the judicial official.
    - Evidence of suspicious behavior, stalking behavior, or research on the personal affairs of the judicial official.
    - Evidence of suspicious behavior, stalking behavior, or research on the personal affairs of the judicial official.
    - Religious and historical themes involving the judicial official (including admonishments for the judicial official to change lifestyle or personal behavior).
    - References to death, suicide, weapons, violence, assassinations, acts of terrorism, or war.

[234] Jenkins, "The U.S. Marshals Service's Threat Analysis Program for the Protection of the Federal Judiciary," 75.

[235] Ibid., 71.

[236] Ibid., 70.

- Expressions of extreme or obsessive admiration or affection.
- Obsessive desire to contact the judicial official (including plans for meetings, interest in home address or other personal information, stalking, surveillance, or following).
- Belief that a debt is owed the person by the judicial official (not necessarily money, but any kind of debt).
- Perception of the judicial official as someone other than himself/herself (an imposter, a historical figure, the suspect's relative, God, or the devil).
- References to public figures who have been attacked (Lincoln, Lennon, Sadat, Kennedy, Judge Vance, etc.).
- References to individuals (or their acts) who have attacked public figures or committed notorious acts of violence or terrorism (Timothy McVeigh, Oswald, Hinckley, Sirhan-Sirhan, etc.).
- References or claims of mental illness, such as psychiatric care, anti-psychotic medication, etc.
- References to bodyguards, security, safety, danger, etc.
- Bizarre or unreasonable solicitations."[237]

While this list is lengthy, such behaviors or communications do not necessarily indicate that criminal activity is occurring or has occurred.[238] Therefore, people engaging in these behaviors may not be detained or arrested as a result.[239] Instead, the presence of these IC&Cs drives the subsequent threat analysis, which is performed by the USMS Analytical Support Unit (ASU).[240] Comparisons are made between the threats at hand and past cases handled by the USMS.[241] The analytical effort seeks to answer three questions:

- "What is it about this communication or contact that resembles previous cases in which the risk escalated?

[237] Jenkins, "The U.S. Marshals Service's Threat Analysis Program for the Protection of the Federal Judiciary," 76–77.

[238] Ibid., 71.

[239] Ibid.

[240] Ibid., 72.

[241] Ibid., 73.

- What is it about this communication or contact that resembles previous cases in which nothing ever happened?
- Is this person likely to act violently based on what is known about the previous cases”?[242]

The analytical process that follows includes public and law enforcement database research to learn as much as possible regarding the suspect and the target.[243] The cases are considered in their totality and judgments made on how to best protect those under the care of the USMS.

3. United States Capitol Police

Also using threat assessment as part of its protective mission, the USCP established a Threat Assessment Section (TAS) in 1989.[244] Charged with protecting the 535 members of the U.S. Congress, the USCP handles this effort somewhat differently than the USSS or the USMS. Specifically, the USCP is centralized in Washington, DC and does not have satellite field offices across the country, as do the USSS and the USMS.[245] In other words, the USCP must establish and rely upon relationships with state and local agencies across the nation to gain assistance with threat cases affecting USCP protectees.[246]

4. Los Angeles Police Department

Behavioral threat management is not exclusive to federal police agencies. Local police agencies also utilize threat management programs and the LAPD has a mature program, created and tailored in the 1990s to counter threats to Hollywood celebrities.[247]

[242] Jenkins, “The U.S. Marshals Service’s Threat Analysis Program for the Protection of the Federal Judiciary,” 74.

[243] Ibid., 72.

[244] Mario J. Scalora and William Zimmerman, “Then and Now: Tracking a Federal Agency’s Threat Assessment Activity through Two Decades with an Eye toward the Future,” *Journal of Threat Assessment and Management* 2, no. 3–4 (2015): 268, doi: 10.1037/tam0000057.

[245] Ibid., 270.

[246] Ibid.

[247] Jeff Dunn, “Operations of the LAPD Threat Management Unit,” *Stalking, Threatening, and Attacking Public Figures*, 2008, 4.

It was established following the investigation of Robert Bardo who murdered actress Rebecca Schaeffer in 1989.[248] The investigation revealed that Bardo, obsessed with Schaeffer, had stalked her by repeatedly approaching and being turned away from television sets where she worked, writing her letters, approaching her manager with the hopes of being introduced to her, and finally, by learning her home address and going there to kill her.[249] Learning from the investigation of Bardo's obsessive approaches of Schaeffer, and her subsequent homicide, led California to adopt the first anti-stalking law in the United States.[250] The new law sought to prevent similar tragedies by criminalizing stalking behaviors.

Similarly, the LAPD determined that it needed to identify ways to prevent stalking and killing of Hollywood celebrities.[251] Established in 1990 to counter such threats, the LAPD Threat Management Unit (TMU) has grown over the years in size and scope to include traditional stalking cases, workplace violence, and terrorism.[252] The TMU also investigates threats to elected officials of Los Angeles.[253] Contrary to traditional reactive policing methods, the emphasis of the LAPD TMU is prevention, leading to new challenges of how success is measured.[254] This experience was shared by the USMS when developing its TAS. It received initial approval from agency commanders for additional funds and resources while also stating that success would mean a reduction in traditional police statistics, such as arrests or mental health commitments used to track police activity.[255] This approach represented a new way of thinking about successful policing.

[248] Jeffrey Dunn, "The Los Angeles Police Department Threat Management Unit," in *International Handbook of Threat Assessment*, ed. J. Reid Meloy and Jens Hoffmann (New York: Oxford University Press, 2014), 285.

[249] Ibid.

[250] Ibid., 286.

[251] Ibid.

[252] Harris and Lurigio, "Threat Assessment and Law Enforcement Practice," 60.

[253] Dunn, "The Los Angeles Police Department Threat Management Unit," 288.

[254] Ibid., 286.

[255] Scalora and Zimmerman, "Then and Now," 269.

As the LAPD broadened its threat assessment priorities, the threat assessment model has likewise been broadly applied, as manifested through consistent growth of membership in ATAP.[256] This non-profit organization was started in 1992 by the LAPD's TMU along with other threat management practitioners, such as law enforcement officers, prosecutors, mental health professionals, and corporate security experts.[257] Its purpose is to afford "its members a professional and educational environment and assessment/intervention techniques, which span all areas of case management. ATAP's goal is to assist our members in becoming better equipped to protect those in need and manage threatening or high-risk situations."[258] Founded in Los Angeles, 14 chapters are now nationwide.[259]

B. EDUCATIONAL INSTITUTIONS AND THREAT ASSESSMENT

The dynamics surrounding threats that occur at schools and institutions of higher learning are no different from threats that occur outside of these environments. Cornell, writing *The Virginia Model for Student Threat Assessment*, points out that previous studies pertaining to school shootings concluded that a useful profile or checklist of potential student attackers could not be identified.[260] Among these studies was the *Safe School Initiative* that was a collaborative research effort between the USSS and the U.S. Department of Education.[261] This research was born in the aftermath of the 1999 mass shooting at Columbine High School and was designed to investigate the thinking,

[256] Douglas Owen Cacialli, "Predicting Problematic Approach Behavior toward Politicians: Exploring the Potential Contributions of Control Theory" (PhD diss., University of Nebraska-Lincoln, 2010, 1, http://digitalcommons.unl.edu/psychdiss/23/.

[257] "About ATAP."

[258] Ibid.

[259] "ATAP Chapters," 2013, http://www.atapworldwide.org/?page=25.

[260] Dewey Cornell, *The Virginia Model for Student Threat Assessment* (Charlottesville, VA: University of Virginia, 2010), 3, http://curry.virginia.edu/uploads/resourceLibrary/Virginia_Model_for_Student_Threat_Assessment_overview_paper_7-16-10.pdf.

[261] Bryan Vossekuil, *The Final Report and Findings of the Safe School Initiative: Implications for the Prevention of School Attacks in the United States* (Collingdale, PA: Diane Publishing, 2002), 3, http://books.google.com/books?hl=en&lr=&id=YYrbptzXMMcC&oi=fnd&pg=PA1&dq=%22and,+%22What+can+be+done+to+prevent+future+attacks+from%22+%22out+school+attacks.+Particular+attention+was+given+to+identifying%22+%22creation+of+safe+environments+for+students,+faculty,+and%22+&ots=pRvBcqY1JY&sig=HJTNTge0IOiEpH3Nhv5IBBYs798.

planning, and pre-attack behaviors of the student perpetrators.[262] The study reviewed cases of targeted violence occurring in U.S. schools between 1974 and 2000.[263] Therefore, the USSS (who conducted the research) recommended that attempts to profile potential school shooters be avoided.[264] Listed as Key Finding 4 in the *Safe School Initiative Final Report,* the researchers concluded that schools should focus their efforts on student behaviors and communications that may indicate attack planning or preparation is underway.[265] Instead, a behavioral threat management approach to preventing school violence was recommended since a number of warning behaviors were identified as part of the research.[266] Most notable among the warning behaviors was leakage. Nearly all the students had communicated their intentions to attack their schools prior to doing so.[267]

Building on the Safe School Initiative, the USSS and U.S. Department of Education, partnered again to create *Threat Assessment in Schools: A Guide to Managing Threatening Situations and to Creating Safe School Climates*.[268] This study reinforced the findings of the Secret Service's Exceptional Case Study Project described earlier, and confirmed that most violent actors did not overtly threaten their targets prior to attacking; instead, they manifested identifiable behaviors before the attacks, that if observed, could have revealed a movement toward the choice to commit targeted violence, and thus, create prevention opportunities.[269]

[262] Vossekuil, *The Final Report and Findings of the Safe School Initiative: Implications for the Prevention of School Attacks in the United States*, 3.

[263] Ibid.

[264] Cornell, *The Virginia Model for Student Threat Assessment*, 3.

[265] Vossekuil, *The Final Report and Findings of the Safe School Initiative*, 34.

[266] Cornell, *The Virginia Model for Student Threat Assessment*, 3.

[267] Ibid.

[268] Robert A. Fein, *Threat Assessment in Schools: A Guide to Managing Threatening Situations and to Creating Safe School Climates* (Collingdale, PA: Diane Publishing, 2002), iii, http://books.google.com/books?hl=en&lr=&id=wHDt1OMyzUYC&oi=fnd&pg=PA9&dq=%22Center+have+found+that+some+school+attacks+may+be+preventable.%22+%22efforts+to+identify,+assess,+and+manage+students+who+may+have+the+intent%22+%22and+public%22+%22personnel,+issues+of+information+sharing,+and+ideas+for+creating%22+&ots=gsXdV5AVmQ&sig=5r1rLLywbCvMS9klbm398FUGKJA.

[269] Ibid., 5.

VI. THE BEHAVIORAL THREAT MANAGEMENT PROCESS

A. MULTI-DISCIPLINARY APPROACHES TO THREAT ASSESSMENT AND MANAGEMENT

As has been described, the LAPD, USMS, USCP, and USSS have threat assessment and management units designed for unique missions. These agencies are large and well-funded. However, many smaller police organizations lack the resources required to stand up similar units to manage threats.[270] Harris and Lurigio recommend alternative remedies for smaller agencies, such as cross-training of officers, mutual-aid agreements, and collaboration with state and federal police agencies.[271]

Jarvis and Scherer emphasize the importance of multi-disciplinary approaches to threat assessment not exclusive to police officers.[272] They also cite the models already in place among the nation's colleges and universities, suggesting these will work well for other organizations seeking to establish assessment and management programs.[273] Hinman and Cook also advocate a multi-disciplinary approach to threat assessment. Discussing the unique circumstances associated with various threats, they observe that professionals from various fields may be more important to certain cases than others.[274] They refer to broad threat assessments needs that include stalkers and domestic abusers, workplace attackers, school shooters, stalkers of celebrities and political leaders, terrorists, and others.[275] Management of threats born out of these various motivations may be improved by utilizing available subject matter experts as part of the team of personnel contributing to the effort.[276]

[270] Harris and Lurigio, "Threat Assessment and Law Enforcement Practice," 66.

[271] Ibid.

[272] Jarvis and Scherer, *Mass Victimization-Promising Avenues for Prevention*, 11.

[273] Ibid., 21.

[274] Dayle L. Hinman and Patrick E. Cook, "A Multi-Disciplinary Approach to Threat Assessment," *Journal of Threat Assessment* 1, no. 1 (2001): 22.

[275] Ibid.

[276] Ibid.

The threat management process is flexible and the totality of the circumstances may change, causing ongoing reevaluation and changes in action, much like the intelligence cycle. Hinman and Cook also note the value of the analysis of intelligence as part of the threat management equation by stating, “Intelligence analysis is critical to the threat assessment process.”[277] They remark that the multi-disciplinary threat management efforts are made more effective when team members may creatively use available intelligence.[278] Analysis may include data collected from the records management systems of police departments, employment data, and motor vehicle data of concerning persons, and other sources.[279]

Scalora and Zimmerman, writing about the history of the USCP Threat Assessment Section, discuss ongoing challenges to the USCP Threat Assessment Section. Highlighting an area in need of attention, they raise the question about when a threat management effort should end once a threatening individual moves out of reach of a specific jurisdiction; with whom should this information be shared, and to whom should third party reports be made?[280] The answer to these questions may exist in the National Network of Fusion Centers.

B. PATHWAYS TO VIOLENCE

The *management* of a threat with a behavioral nexus follows the initial assessment of the threat. It is the portion of the process describing the efforts by which a person may be steered, directed, or led away from the commission of a violent act. Using the “pathway to violence” metaphor as a mechanism to understand this process, intended violence is best understood as a process that is an amalgamation of what Calhoun and Weston describe as “discreet, sequential, recognizable behaviors.”[281] This pathway may be visualized in Figure 1.

[277] Hinman and Cook, “A Multi-Disciplinary Approach to Threat Assessment,” 26.

[278] Ibid.

[279] Ibid., 27.

[280] Scalora and Zimmerman, “Then and Now,” 274.

[281] Calhoun and Weston, *Contemporary Threat Management*, 57.

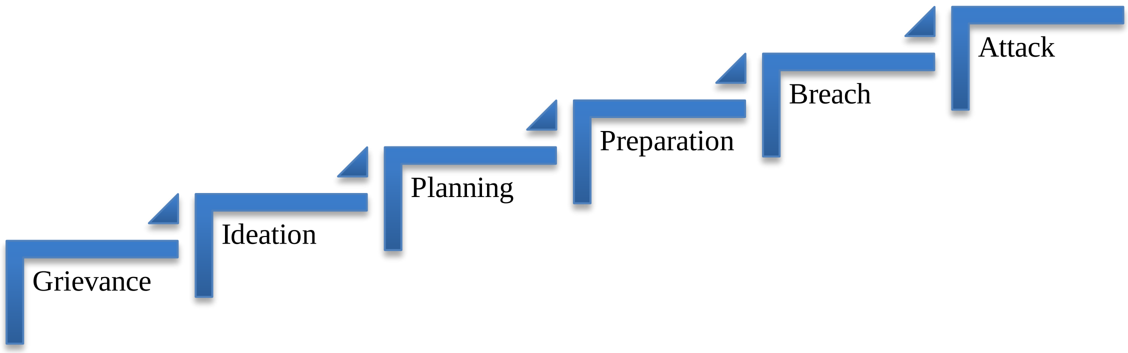

Figure 1. Path to Intended Violence.[282]

Once a threat has been assessed for the first time, a threat management strategy should be developed based upon whether or not the threatening subject has been deemed to be moving toward or away from a violent attack.[283] Ideally, a multi-disciplinary team that regularly interacts and works together creates the management strategy.[284] The multi-disciplinary approach is used today in college and university settings but is also recommended for broader use, outside of academic environments.[285] As previously noted, threat management is used by a host of police agencies. Utilization of a formal process to assess and manage threats is imperative, regardless of the specific composition of a threat management team.[286] A structured process fosters common awareness of cases being managed while ensuring that appropriate attention and context is being applied.[287] It also improves the awareness of case management supervision, allowing for opportunities to observe and reassess the management process over time.[288] Application

[282] Adapted from Calhoun and Weston, *Contemporary Threat Management*, 58.

[283] Fein, Vossekuil, and Holden, *Threat Assessment: An Approach to Prevent Targeted Violence*.

[284] Gene Deisinger et al., *The Handbook for Campus Threat Assessment Teams* (Stoneham, MA: Applied Risk Management, LLC, 2008), 12.

[285] Jarvis and Scherer, *Mass Victimization-Promising Avenues for Prevention*, 21.

[286] Ibid., 23.

[287] Ibid.

[288] Ibid.

of such a process ultimately contributes to the management team's ability to offer a structured professional judgment.[289]

As behavioral threat assessment has evolved, it has been suggested that the intelligence cycle may be an effective tool by which to assess and manage behavior-based threats of targeted violence.[290]

C. THE INTELLIGENCE CYCLE AND THREAT ASSESSMENT AND MANAGEMENT

Figure 2 is a representation of what is commonly known as the intelligence cycle. It helps visualize the process by which information becomes intelligence through analysis.

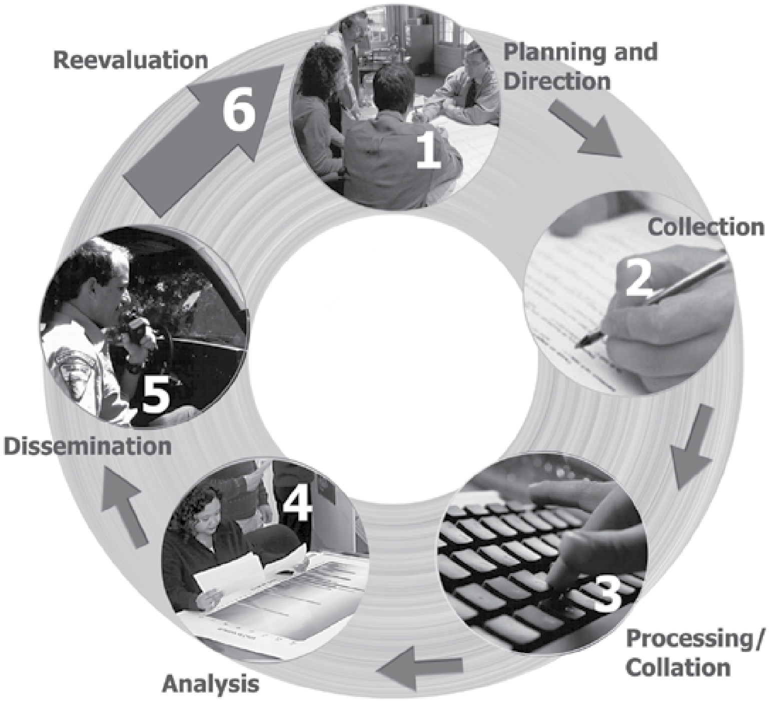

Figure 2. The Intelligence Cycle.[291]

[289] Meloy et al., "The Role of Warning Behaviors in Threat Assessment," 275.

[290] Rick Malone, "Protective Intelligence: Applying the Intelligence Cycle Model to Threat Assessment," *Journal of Threat Assessment and Management* 2, no. 1 (March 2015): 61.

In this process, raw information is developed into finished intelligence for use by decision makers.[292] Utilized for protective intelligence matters, the intelligence cycle is effective because it satisfies the need for continuous feedback and reassessment.[293] Threat management strategies require feedback and reassessment and may be classified as non-confrontational and confrontational.[294] While labeled this way for convenience, the threat management process does not require that one approach be selected to the exclusion of the other.[295] The choices are informed by the ongoing collection and analysis of the evolving circumstances. Further, action or inaction taken by a threat manager will either make the situation better, worse, or produce no change.[296] Hence, a need always exists for new and improved information and analysis.

At this juncture, the planning and direction of the intelligence cycle serves the threat management process.[297] Next, the collection of information for analysis is required. Three types of information are useful: human intelligence or HUMINT, geospatial intelligence or GEOINT, signals intelligence or SIGINT, and open source intelligence or OSINT.[298] Each has value, but for the threat assessment and management team, HUMINT and OSINT are most impactful.[299]

Noted in the *Baseline Capabilities for State and Major Urban Area Fusion Centers*, the nation's fusion centers use the intelligence cycle and OSINT to collect information and conduct intelligence analysis.[300] OSINT is intelligence gleaned from

[291] Source: Criminal Intelligence Coordinating Council, *Fusion Center Guidelines*, 19.

[292] Ibid., 20.

[293] Malone, "Protective Intelligence: Applying the Intelligence Cycle Model to Threat Assessment," 54.

[294] Calhoun and Weston, *Contemporary Threat Management*, 183.

[295] Ibid., 185.

[296] Calhoun and Weston, *Contemporary Threat Management*, 189.

[297] Malone, "Protective Intelligence: Applying the Intelligence Cycle Model to Threat Assessment," 54.

[298] Ibid., 55.

[299] Ibid.

[300] United States Department of Justice, *Baseline Capabilities for State and Major Urban Area Fusion Centers*, 19.

publicly available information, collected without special legal permissions or covert techniques.[301]

The applicability of the intelligence cycle to threat management was discussed earlier. As noted in the *Fusion Center Guidelines*:

> The principal role of the fusion center is to compile, analyze, and disseminate criminal/terrorist information and intelligence and other information (including, but not limited to, threat, public safety, law enforcement, public health, social services, and public works) to support efforts to anticipate, identify, prevent, and/or monitor criminal/terrorist activity.[302]

Based upon this description, and the duties set forth to adjudicate threats, the argument may be proffered that fusion centers should adopt protocols by which to conduct behavioral threat assessments and management techniques.

Step six of the current intelligence cycle recommended for use by fusion centers requires "reevaluation."[303] Reevaluation serves the threat assessment and management process by taking new or developing information into account and informing decision makers, such as a threat management team. Building on the reevaluation step, producers of analytical products frequently offer statements that help their consumers gauge the degree of confidence that should be attached to an analytical product by employing statements of "analytic confidence."[304]

[301] Carter, *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies*, 63.

[302] Criminal Intelligence Coordinating Council, *Fusion Center Guidelines*, 13.

[303] Criminal Intelligence Coordinating Council, *Fusion Center Guidelines*, 19.

[304] Malone, "Protective Intelligence: Applying the Intelligence Cycle Model to Threat Assessment," 57.

VII. ANALYSIS: FUSION CENTER INTEGRATION

A. FUSION CENTER OPERATIONS AND THREAT MANAGEMENT

Since the need to address threats of mass or targeted violence presents significant challenges to domestic law enforcement agencies, fusion centers may be well positioned to support the effort to prevent such acts. The U.S. Congress has defined the term "fusion center" to mean a "collaborative effort of 2 or more Federal, State, local, or tribal government agencies that combine resources, expertise, or information with the goal of maximizing the ability of such agencies to detect, prevent, investigate, apprehend, and respond to criminal or terrorist activity."[305] Herein, the objective of fusion centers is to minimize informational silos to enhance information sharing and collaboration.[306]

Likewise, behavioral threat assessment represents an effort to identify where information about a threat may exist and also break down any silos that hinder the flow of information to those who must collect and share it.[307] This process is intuitive for fusion centers, as most are already engaging in similar processes to evaluate and manage suspicious activity reports relative to terrorism and other crimes.[308]

Unlike the law enforcement agencies described earlier, fusion centers across the country do not currently have nationally coordinated or tailored responsibilities when it comes to behavioral threat assessments or management strategies. However, the all-hazards-all crimes missions of fusion centers adopted by many centers means that they have been encouraged to avoid any limitation of their analytical focus upon specific areas

[305] 110th Congress, *Implementing Recommendations of the 9/11 Commission Act of 2007,* 121 STAT. 266, 2007, 322 (Washington, DC: Government Printing Office, 2007), https://www.nctc.gov/docs/ir-of-the-9-11-comm-act-of-2007.pdf.

[306] National Fusion Center Association, *National Strategy for the National Network of Fusion Centers*, 24.

[307] Deisinger et al., *The Handbook for Campus Threat Assessment Teams,* 5.

[308] "Nationwide SAR Initiative (NSI)—About the NSI."

of the threat spectrum at the exclusion of others.[309] Instead, they must address all the varying threats coming to their attention. However, this broad approach may actually improve the overall effectiveness of fusion centers when dealing with threats since many threats are not related to international terrorism but still require attention to prevent violence.

The National Fusion Center Association produced a national strategy document in 2014 to guide the continuing evolution of the nation's 78 fusion centers through 2017. Within this document, the need to address matters relative to the management of cyber threats was articulated.[310] While the need to dedicate time and analytical effort in the pursuit of behavioral threats is not specifically mentioned, the strategy does say that "because violent crime and terrorism are threats to our nation, the specialized knowledge, skills, abilities, and experience of one center must be available to all centers, while the increased capacity and analytical capability of the National Network must be available to all governors and major urban areas."[311]

As fusion centers have evolved since their inception following the terror attacks of 9/11, opportunity exists to leverage their capabilities to help manage the variety of threats that come to their attention. These threats may be presented in traditional ways (phone, letter, email) or through contemporary communication methods, such as social media. Such threats are likely to be handled in different ways across the decentralized fusion center network since each center has its own policies and priorities.[312]

Common threats are specific behaviors manifested by potential attackers before acts of violence are carried out. Identifying and understanding these behaviors may allow

[309] George W. Bush, *National Strategy for Information Sharing: Successes and Challenges in Improving Terrorism-Related Information Sharing* (Bloomington, IN: Wordclay, 2009), A1-1, http://books.google.com/books?hl=en&lr=&id=vEJbUn3nQ4cC&oi=fnd&pg=PA1&dq=%22the+sharing+of+information+across+all+levels+of+government,+disciplines,+and%22+%22Strategy+was+developed+with+the+understanding+that+homeland+security+information,%22+%22of+funding+and+other+resources+for+homeland+security-related%22+&ots=PJfoeP_WAO&sig=SBNmmgke3w5qtlMUd3IUyxHDdF0.

[310] National Fusion Center Association, *National Strategy for the National Network of Fusion Centers*, 28.

[311] Ibid., v.

[312] Ibid., 9.

fusion centers to provide greater service and value to their stakeholders. Further, behavioral threat management strategies exist. Fusion centers may be able to facilitate such strategies for the purpose of preventing mass or targeted violence. A behavioral threat assessment and management model to be used by fusion centers may be replicated from those that exist elsewhere in law enforcement or school settings. Therefore, a threat management approach may be valuable to the National Network of Fusion Centers.

The investigation and management of threats is most likely to be successful if agencies or systems beyond the realm of law enforcement are identified and used to help manage problems associated with a particular case.[313] Fusion centers then offer opportunities to serve as the organizations that have the relevant relationships with the various entities required to manage threats successfully. Among these include, but are not limited to, prosecutors, probation and parole offices, correctional agencies, employee assistance services, victim's advocacy services, community groups, and others.[314] Fusion centers are also expected to work with public safety organizations, such as emergency management agencies, public health agencies, social services agencies, public works agencies, and the private sector.[315] Notwithstanding that the foundation of fusion centers is grounded in the law enforcement intelligence function, it is recommended in the *Fusion Center Guidelines* that certain functional categories exist to maximize the effectiveness of the fusion process.[316] These categories extend well beyond the traditional scope of law enforcement interest and illustrate the all-hazards-all crimes analytical priorities of contemporary fusion centers. As compiled by the Criminal Intelligence Coordinating Council, these include the following.

- agriculture, food, water, and the environment
- banking and finance
- chemical industry and hazardous materials

[313] Fein, Vossekuil, and Holden, *Threat Assessment: An Approach to Prevent Targeted Violence*, 3.

[314] Ibid.

[315] Criminal Intelligence Coordinating Council, *Fusion Center Guidelines*, 3.

[316] Ibid.

- criminal justice
- education
- emergency services (non-law enforcement)
- energy
- government
- health and public health services
- hospitality and lodging
- information and telecommunications
- military facilities and defense industrial base
- postal and shipping
- private security
- public works
- real estate
- retail
- social services
- transportation[317]

Indeed, the integration of this wide variety of sectors into the operations of fusion centers establishes an ideal by which each level of government, the private sector, and the public can make contributions to the fusion process.[318] Maximizing the variables (agencies and corresponding knowledge) being incorporated into the fusion process increases the overall quality of the analytical output of a fusion center.[319]

The *Fusion Center Guidelines* present law enforcement intelligence as a phase of intelligence necessary to support fusion center operations.[320] Thus, intelligence is defined

[317] Criminal Intelligence Coordinating Council, *Fusion Center Guidelines*, 3.

[318] Ibid.

[319] Ibid., 29.

[320] Ibid., 15.

as being the "product of systematic gathering, evaluation, and analysis of raw data on individuals or activities suspected of being, or known to be, criminal."[321]

As the *Fusion Center Guidelines* recommend diverse input into the intelligence process, a similar approach is advocated for successful behavioral threat management, which is often observed in the literature as a "multidisciplinary approach." Time has been spent discussing the threat management process and the stages of threat management to include the identification of threats, assessment of threats, and management of those who pose threats.[322] Accomplishing this process requires a comprehensive analysis of a host of variables to include warning behaviors, as well as environmental triggers that may add to someone's proclivity to become violent, or to steer away from violence.[323] This approach allows for the management of threat cases instead of mere risk assessments or profiles.

B. APPLIED THREAT MANAGEMENT—THE VIRGINIA FUSION CENTER

The author of this thesis is the director of the Virginia Fusion Center (VFC). The following information and examples are offered from his personal experience serving in this capacity. Beginning in 2014, the VFC recognized a need to develop a formal process by which to handle threats. Thus, it began developing a behavioral threat assessment and management protocol for use by the center. Born out of the need to handle a diverse variety of threats coming to the attention of the VFC, the policy development process involved research and interviews with subject matter experts at the USSS, USCP, the USMS, and the Virginia Tech Police Department.

Since that time, the VFC has been requested to assist with a number of incidents requiring the analysis of threats with a behavioral context. Two examples are offered as follows to illustrate the manner by which a fusion center may support its stakeholders by

[321] Criminal Intelligence Coordinating Council, *Fusion Center Guidelines*, 15.

[322] Harris and Lurigio, "Threat Assessment and Law Enforcement Practice," 56.

[323] Ibid.

utilizing the behavioral threat management approach to prevent mass or targeted violence.

1. Example 1—Potential Workplace Violence Averted

During the spring months of 2016, the VFC received a request from a state correctional agency. After learning his employment probationary period would continue for another six months beyond the customary end, an employee of the agency abruptly resigned his employment and sent a series of threatening emails from his personal email account to his former managers expressing grievances and dissatisfaction with having his probation extended. The agency failed to collect the identification credentials upon the employee's separation, so concern developed that he may attempt to enter the facility and harm his former coworkers or managers. This concern was founded in the totality of numerous warning behaviors that were considered. Among these were *fixation*, *leakage*, *directly communicated threat*, *identification*, *last resort* and *pathway* warning behaviors.

These behaviors became manifest in the former employee's expressions of grievances via email to his former employers coupled with sightings of him driving slowly through the parking lot of his old office while staring at the office. These emails were riddled with profanity, as well as threatening language emphasizing the subject's grievances.[324] The subject expressed blame directed toward his former supervisors and coworkers for the downturn in his career and the perceived impact on his life followed with a declaration that he was out of options and was now focusing on them for revenge.[325]

Even though the language was threatening, but the VFC had to judge whether or not it was that of a "hunter" or a "howler" and whether or not the subject was merely making threats or if he posed a threat. The emails represented *leakage* warning behaviors, as well as *directly communicated threat* warning behaviors.[326] The acts of driving to his

[324] Virginia Fusion Center, *Information Report, Threat Assessment* (Richmond, VA: Virginia Fusion Center, April 29, 2016).

[325] Ibid.

[326] Meloy et al., "The Role of Warning Behaviors in Threat Assessment," 266.

former workplace on multiple occasions and observing the building and surroundings represented *fixation* warning behavior.[327] Context was necessary; thus, more information was needed. As noted by Meloy et al., “warning behaviors in this context are intended to be used as indications of a recent or current significant increase in risk which requires a response.”[328]

Meetings between the VFC and the correctional agency’s security personnel were held to develop a strategy to prevent the subject from engaging in violence. It was learned during these initial meetings that the subject had a host of personal challenges including a recent divorce, financial stress, previously sought mental health services, was taking medication for depression, and was abusing alcohol. These circumstances may have been indicative of *pathway* warning behavior.[329] He had extensive experience with weapons as a member of the U.S. military and the corrections field as a guard and probation officer. He recently sold his personal vehicle to buy firearms, also potentially indicative of *pathway* warning behavior.[330] The VFC also learned that the subject was fond of posting images of himself to social media sites that portrayed him in apparel similar to that which is associated with outlaw motorcycle gangs (OMGs) while seated upon a Harley Davidson motorcycle. The subject donned a heavy leather vest (also known as a “cut”) adorned with assorted patches, motorcycle boots, and dark wrap-around sunglasses. These actions may have been indicative of *identification* warning behavior if the intent was to appear menacing or aggressive.[331] Again, context was required for clarity.

The VFC took the following threat management actions in the effort to prevent the subject from engaging in violence. When first presented with the case, the VFC had to determine whether or not the subject presented an imminent threat to others that would require a law enforcement response to take him into custody immediately.[332] This step is

[327] Meloy et al., “The Role of Warning Behaviors in Threat Assessment,” 265.

[328] Ibid., 274.

[329] Ibid., 265.

[330] Ibid.

[331] Ibid.

[332] Deisinger et al., *The Handbook for Campus Threat Assessment Teams*, 53.

recommended for all threat management teams to help mitigate cases that have come to the attention of threat managers too late for management strategies to work or have progressed too quickly for contemporary threat management strategies to be attempted due to the imminence of the threat against a target.[333]

- Consideration was given to whether or not judicial orders of protection should be issued on behalf of the correctional agency staff who had been threatened. While this step may seem intuitive to take, securing an order of protection requires the order be served on the person making the threat. Law enforcement personnel handle service of such an order in Virginia. The act of serving legal process upon someone who is the subject of a threat management case may have negative consequences if the subject feels humiliated, belittled, or bullied as a result, leading to the conclusion that no options remain except violence.[334] This situation is known in behavioral threat assessment parlance as a "triggering event" and may be something that causes subjects to take some action that furthers their progression toward violence.[335]

- The VFC arranged for a site survey of the agency facility by a crime prevention specialist of the VFC. Recommendations were made pertaining to security enhancements.

- Armed security was recommended for the exterior of the correctional facility to detect and prevent approaches by the former employee.

- The VFC issued an officer safety bulletin to state and local law enforcement personnel in the region to make them aware of the subject and the circumstances associated with his threats.

- Notwithstanding the concern associated with creating a triggering event, an emergency protective order was recommended so that the subject could be taken into custody to be evaluated by mental health professionals. Like the order of protection, this step must be carefully considered because such orders usually expire after 72 hours and may lead subjects to conclude that they can only settle the grievance through violence as a last resort. In this case, the protective order was deemed necessary due to the totality of what was known about the subject coupled with the content and nature of his threatening communications. Prior to service of the order, the VFC held a conference call with the correctional agency and the Sheriff's Department tasked with serving it to help prevent the process of taking the

[333] Deisinger et al., *The Handbook for Campus Threat Assessment Teams*, 53.

[334] De Becker, *The Gift of Fear*, Kindle location 2675.

[335] Denise Bulling and Mario Scalora, "Threat Assessment Glossary," 18, 2013, http://digitalcommons.unl.edu/publicpolicypublications/123/.

subject into custody from becoming a catalyst for violence. The Sheriff's Department selected a deputy specially trained in crisis intervention to make the approach and contact the subject. The deputy was briefed by the VFC and the correctional staff managing the case and provided with important context regarding the subject to reduce the potential for violence when the subject was physically taken into custody.

- The consultation between the VFC and the Sheriff's Department paid dividends. The responding deputy made contact with the subject, established a rapport with him, gained entry in his residence, and made observations regarding the subject's living conditions and habits. This information helped inform mental health providers who would triage the subject later. Most importantly, the responding deputy knew how to handle the subject due to the background information with which he was provided and the crisis intervention training he possessed.

- Following the initial actions taken by the VFC, Sheriff's Office, and the correctional agency, a longer-term threat management plan was created and implemented. This plan also included publicly funded mental health providers in the subject's area and voluntary efforts on the part of the subject to seek their services.

- This case was particularly challenging because the subject had almost no social support network except for the relationships he developed after this incident. These relationships included the deputy with crisis intervention training and a security staff member with the correctional agency. Ironically, those who might initially be perceived by the subject as persecutors became trusted advocates.

- As of this writing, six months have passed, the threatening communications have ceased, and the subject continues to be periodically contacted by those from the Sheriff's Office and correctional agency to ensure that he is functioning well.

2. Example 2—Potential Targeted Violence Averted

During the spring of 2016, another state correctional organization contacted the VFC concerning threats made by an inmate who was about to be released from incarceration. It was reported that the inmate wished to avenge a sibling who was incarcerated elsewhere in Virginia by murdering the prosecutor and judge who prosecuted and convicted the sibling, resulting in a long jail sentence. The threats were reported to authorities by another inmate with access to the subject of this case.

The reporting inmate also indicated that the subject inmate stated that he intended to kill the judge who sentenced his sibling, as well as the prosecutors and their family members. He added that he had experience with sniper weapons and hand-to-hand combat tactics as a U.S. Marine for five years.[336] These statements represent *leakage* warning behavior since they were uttered in confidence to another inmate.[337] They also indicate the possibility of *identification* warning behavior, considering the affinity expressed for the military and weapons while in the context of this threat.[338]

It was also learned that while still incarcerated, the inmate sent letters to the judge and prosecutor several years before his release date. The letters did not contain overt threats but instead contained the phrase "car accident" written in excess of 80 times in each letter, followed by the phrase "good luck."[339] These statements may represent *leakage* or *fixation* warning behaviors.[340]

Since the inmate had served the balance of his sentence, the correctional agency had no legal recourse to continue his incarceration. His imminent release caused concern among state and local authorities since Virginia's judges typically operate without protective details and may be vulnerable to attack. The VFC coordinated with the correctional agency, law enforcement officials in the geographic area where the subject was incarcerated, and those in the area where he was to be released. The VFC also contacted the probation and parole officials who would be responsible for managing the subject while on supervised probation after his release. Assisting in these efforts was the USMS who provided expertise in judicial protection.

Based upon the identifiable warning behaviors, the VFC determined that more information and context was necessary. It hosted a series of conference calls with the aforementioned organizations to gather all pertinent information pertaining to the subject

[336] Virginia Fusion Center, *Information Report, Threat Assessment* (Richmond, VA: Virginia Fusion Center, May 20, 2016).

[337] Meloy et al., "The Role of Warning Behaviors in Threat Assessment," 265–266.

[338] Ibid., 265.

[339] Virginia Fusion Center, *Information Report, Threat Assessment*, May 20, 2016.

[340] Meloy et al., "The Role of Warning Behaviors in Threat Assessment," 265.

and his pending release. For example, during one call, it was reported by the local law enforcement agency that its records management system was queried for activity at the address where the inmate was to be settled upon release. It was revealed that a juvenile member of the household and relative of the inmate had recently been accused of bringing a firearm to school and making threats toward a specific student. Concern developed that the inmate may be introduced to an unstable environment with access to firearms upon release. Another example of developments that caused the threat management strategy to change involved the interception of jailhouse communications between the subject and his mother. These conversations revealed that the subject intended to move his residence upon release without making his probation officer aware.

Each call shed light on limitations and opportunities regarding each stakeholder agency. Based upon the information received during each call, coupled with records provided by the correctional agency, a threat assessment was conducted regarding whether or not the subject posed a threat to his sibling's prosecutor, the convicting judge, or others. Working with the other agencies that had a role in this case, the VFC crafted a threat management strategy that was adopted and modified with each conference call. Hence, comparisons to the intelligence cycle are relevant as the VFC updated its threat assessment and guidance to those managing the subject in the field. Utilizing the behavioral threat assessment model allowed the VFC to incorporate structure in the analysis it provided to stakeholders, which is deemed preferable to the expert opinion offered by a single consultant.[341]

The VFC incorporated the *directly communicated threat* warning behavior with other variables to make its analytical judgment.[342] These variables included information received from the mental health professionals who had interacted with the subject while incarcerated, records of the subject's conduct while incarcerated, his criminal record, his military record, and other institutional measures taken of the subject utilized by the institution to manage him while incarcerated. The analytical judgments changed as the

[341] Malone, "Protective Intelligence: Applying the Intelligence Cycle Model to Threat Assessment," 56.

[342] Meloy et al., "The Role of Warning Behaviors in Threat Assessment," 265.

environmental variables affecting the inmate’s discharge and home plan changed. The threat management plan was developed in conjunction with the probation and parole personnel, the law enforcement agency where the subject would be living post-release, and the social services and mental health providers, representing a multi-disciplinary approach that helped inform the overall management strategy.[343]

The subject was released after multiple years of incarceration. Based upon the threat management strategy facilitated by the VFC, deliberate steps were taken to manage him to ensure he did not progress along a pathway to violence while still respecting his civil rights and civil liberties as a citizen of Virginia and the United States. As of this writing, five months have passed with no violent attempts against those whom he previously threatened. The probation and parole staff is intensively supervising the subject in cooperation with mental health providers.

3. Example 3—Potential Campus Shooting Averted

This final example from the VFC involves a male subject who attends a public university in Virginia. The subject first came to the attention of the VFC in mid-November 2016. A Virginia State Police trooper sent a suspicious activity report to the VFC based upon recent contact with a local firearms retailer with whom the trooper had frequent contact. The retailer called the trooper to relay an incident that took place in his shop earlier in the day.

A male in his late teens had entered the store and requested to look at several semi-automatic magazine-fed rifles similar in appearance to military assault weapons. The man then settled on a semi-automatic version of an AK-47 rifle and indicated that he wished to purchase it with cash. The storeowner told the man that he reserved the right to refuse sale of the weapon to anyone less than 21 years of age. Hearing this, the customer immediately lost his temper and began shouting at the shop owner. The customer then left the store, got into the car that had brought him, and went to another gun shop located across the street. He went inside the second gun shop but immediately left without making a purchase and left with the person who had driven him there. It was later learned

[343] Hinman and Cook, “A Multi-Disciplinary Approach to Threat Assessment,” 24.

that the subject saw a uniformed police officer in a patrol car near the second gun shop and hastily left without attempting a purchase.

As a result of the person's unusually aggressive behavior in the first store, the shop owner called the trooper to make notification of the incident, providing a description of the man and the license plate of the car in which he had been riding. The trooper determined that the driver of the car was an Uber driver and the person who had secured the ride was not the same person who rode in the car to the store because the Uber account holder was female. The Uber driver was located and interviewed. He stated that he had picked up the young male who had then asked to be taken to the nearest gun store. The male offered the Uber driver $100 cash tip if he waited for him while he attempted to purchase the rifle. The male also revealed that he was from another state and wanted the rifle due to protest activities subsequent to the U.S. presidential election.

At this point, the VFC was notified. The VFC reviewed the SAR and notified the FBI's Joint Terrorism Task Force (JTTF) task force officer also assigned to the VFC. A second Virginia State Police special agent was also called to assist. The matter was investigated and the Uber account holder was identified and interviewed. She indicated that she ordered the ride for the man because the subject told her that he needed a ride and offered to reimburse her with cash. Surveillance images from the first gun shop led to the identification of the man of concern. The investigation also revealed that the man had been the subject of a criminal investigation where a search warrant was served on his university apartment earlier in the day by local police officials. Therefore, the man had his apartment searched and vehicle seized by police officers only a few hours before he entered the gun shop and attempted to purchase a semi-automatic military style rifle.

The investigation continued and the man agreed to a consensual interview with two Virginia State Police special agents assigned to the VFC. Little was learned, as the man was reluctant to discuss his circumstances or reasons for attempting to purchase the rifle. Further investigation into open source information pertaining to the subject led investigators to conclude that he had a number of stressors influencing him. Among these were the recent deaths of his parents (2009 and 2015, respectively), the break-up of a romantic relationship, being subject to a criminal investigation in Virginia, having criminal charges pending against him in another state, having little social or familial support, and substance abuse.[344]

Unlike the previous examples, this case lacked an abundance of warning behaviors. The subject did not frequently use social media and his accounts were not current. During the criminal investigation, his smartphone was seized and a search warrant was obtained for its contents. However, police investigators could not break the encryption; thus, an opportunity to detect any potential warning behaviors or criminal activities was lost. The attempt to purchase the AK-47 type of rifle may have been an attempt to adopt a pseudo-commando persona, possibly representing *identification* warning behavior since the AK-47 rifle is used by many of the world's militaries, terror groups, and other militant organizations.[345] However, it was not a strong conclusion since the choice of the weapon style was not actually known and a structured conclusion could not be reached without more information.

Since warning behaviors were not immediately available for observation, a collaborative effort was pursued to collect and analyze all the individual pieces to obtain a more comprehensive understanding of the subject and how to manage him. Since it was learned that the subject lived in university housing, had used a third party to secure the Uber ride to the gun store shortly after the police served a search warrant on him, had become outwardly angry upon being denied the opportunity to purchase the firearm, and because he was already under criminal investigation, the VFC concluded that sufficient concern existed for continued follow-up. The VFC began communicating with the campus police department and the university threat assessment team for the purpose of developing a threat management strategy to help the subject steer away from violence. The Commonwealth of Virginia requires all publicly funded schools have threat assessment teams for the purpose of assessing and preventing violence on school

[344] Virginia Fusion Center, *Information Report, Threat Assessment* (Richmond, VA: Virginia Fusion Center, November 14, 2016).

[345] "Russian/USSR Military AK-47," accessed November 26, 2016, http://www.guns.com/reviews/Russianussr-military-ak-47/.

grounds.[346] Therefore, the university already had a dedicated team of people who understood the threat management process and they immediately engaged with the campus police and the VFC threat management personnel.

The threat management team met and included the VFC staff assigned to the case, as well as the campus police department. Management strategies were crafted to help steer the subject away from a short-term interest in purchasing a firearm while also attempting to identify stabilizing forces in his life to help him consider alternative choices to violence.[347] These strategies involved the utilization of campus counseling services and social networks outside of school.[348] Extended family members were identified in other states and interviewed by law enforcement personnel in those areas.[349] This process took several days.

Six days later, the subject presented himself to another gun dealer in a different area near the university. He asked to see a rifle and one of the store attendants showed him a more traditional bolt-action style rifle. When the subject completed the paperwork for the background check prior to purchasing the weapon, the dealer told him that the check was not instant and he may have to wait a few minutes to get the results. Instead of waiting, the subject left the store, but without further communicating with the staff. He did not return. Later, the same dealer received a notice from the Virginia Firearms Transaction Center that the subject was not eligible to make the transaction due to a pending criminal charge against him in another state. This event was reported to a Virginia State Police trooper by the gun store and it was quickly realized that subject of the threat management investigation had again attempted to purchase a firearm.

Concern among the threat assessment team grew since the determination to buy a rifle did not appear to have abated. This development led the campus threat assessment team, university police department, and personnel from the VFC to have another threat

[346] "Threat Assessment Teams and Oversight Committees, Code of Virginia, vol. 22.1-79.4," 2013, http://law.lis.virginia.gov/vacode/title22.1/chapter7/section22.1-79.4/.

[347] Virginia Fusion Center, *Information Report, Threat Assessment,* November 14, 2016.

[348] Ibid.

[349] Ibid.

management meeting to discuss the new development and make determinations about what the next steps would be for the subject.[350] It was considered whether or not the school and the subject were best served by having the school exercise the option to remove him from the academic program and university housing due to the criminal investigation into his activities while in the school's housing, compounded with his refusal to respond to outreach efforts to help him. The subject's extended family members were also made a part of the process to manage his behavior. One family member who had strong rapport with the subject agreed to attempt to broker a resolution whereby the subject would accept counseling services and be allowed to remain on campus and in classes. However, he was rebuffed. The threat management team identified a previous counselor who had a good relationship with the subject and asked for his assistance with the management effort. The counselor was able to persuade the subject to go out of town with family members for an upcoming long weekend and accept a psychological evaluation upon his return.

The VFC prepared a situational awareness bulletin for the state where the subject would be headed for a long weekend, as well as the states through which the subject would pass. This report was sent to the fusion centers of these states for the purpose of providing some background information should the police encounter the subject for some reason and need additional context or information. It would also allow the local campus threat management team, through the VFC, to have visibility on such circumstances should they occur outside of Virginia. As of this writing, the long weekend away from the university is underway and the management of the subject continues.

During this latter stage of the threat management process, the VFC played an important role in conveying the fluidity of the situation to partner agencies in other states that would not otherwise know about the circumstances of the threat management effort occurring in Virginia. This scenario illustrates the maturity of the network, as well as its utility when handling tactical-level issues. The threat assessment process may be the

[350] Virginia Fusion Center, *Information Report, Threat Assessment*, November 14, 2016.

opportunity for fusion centers to connect elements of issues that would have not have been connected prior to their establishment.

THIS PAGE INTENTIONALLY LEFT BLANK

VIII. RECOMMENDATIONS AND CONCLUSION

A. CHALLENGES AND OPPORTUNITIES—TRAINING

It has been argued in this thesis that fusion centers may operate more proactively by incorporating the Behavioral Threat Assessment and Management model as a tool by which to prevent mass or targeted violence. However, no plug-and-play training solution is available for fusion centers to begin. A host of opportunities exist to train personnel and create programs to do this work, but nothing as yet exists specifically for fusion centers.

Also lacking is a common framework for the development of threat assessment and management procedures to be used in fusion centers. At this time, the experiences of agencies that have been performing this function are of the best value to fusion centers that wish to develop this capability. Among these agencies are the USSS, USCP, USMS, and the LAPD.

The DHS, partnering with the Department of Justice's Bureau of Justice Assistance, created a technical assistance program in 2007 designed to support fusion centers through a host of developmental requirements.[351] These programs provide basic training in fusion center operations, fusion center management, SAR, privacy and civil liberties, critical thinking, integration of technology, and others.[352] However, training is not yet dedicated to behavioral threat assessment and management. The closest technical assistance topic area is that of SAR since the vetting of behaviors (or the lack thereof) is an important element.[353]

Lacking a centralized federal training program, where does this leave everyone regarding guidance for fusion centers to begin conducting behavioral threat assessments and manage cases? Behavioral threat assessment and management conducted by a police

[351] U.S. Department of Homeland Security and U.S. Department of Justice, *DHS/DOJ Fusion Process —Technical Assistance Program and Services* (Washington, DC: United States Government, 2014), 4, https://www.ncirc.gov/documents/public/Fusion_Process_catalog_of_services_version_8.pdf.

[352] Ibid., 5–7.

[353] Ibid., 31.

agency, a college threat assessment and management team, or a fusion center, is different from traditional policing methodologies in that it does not seek to punish or aggressively confront those who manifest behaviors of concern.[354] Performed with the objective of preventing targeted violence, the process endeavors to assist people who may be posing threats to others or those who are being threatened.[355] Like any new operational development, establishing a threat assessment and management program requires basic and advanced training.[356] Professionals who possess relevant qualifications related to threat assessment and management may deliver this sort of training.[357]

Basic training may take the form of webinars, conferences, workshops, or other presentations, delivered by professionals in the field of threat assessment and management.[358] Further, building beyond basic capabilities, advanced training may take the form of tabletop exercises or other practical scenario-based training, administered by subject matter experts in the field of threat assessment and management, allowing participants to work through realistic scenarios and receive relevant feedback and guidance.[359] These courses are currently offered in the private sector to help individuals and organizations establish their capabilities.[360]

ATAP created a program in 2015 for interested persons to become certified threat managers.[361] Backing the certification with ATAP's status as a professional organization, baseline professional capabilities are established by which to measure a common standard of quality for someone to present a certification.[362] This certification requires a

[354] Deisinger et al., *The Handbook for Campus Threat Assessment Teams*, 25.

[355] Ibid.

[356] Marisa Randazzo and Ellen Plummer, *Implementing Behavioral Threat Assessment on Campus—A Virginia Tech Demonstration Project* (Blacksburg, VA: Virginia Polytechnic Institute and State University, 2009), 26, https://www.threatassessment.vt.edu/Implementing_Behavioral_Threat_Assessment.pdf.

[357] Deisinger et al., *The Handbook for Campus Threat Assessment Teams*, 98.

[358] Ibid.

[359] Ibid.

[360] "Training," accessed November 16, 2016, http://www.sigmatma.com/law-enforcement-security/training/.

[361] "Certified Threat Manager," 2015, http://www.atapworldwide.org/default.asp?page=CTM.

[362] Ibid.

comprehensive examination of the candidates' understanding of the current "body of knowledge" that exists in the academic literature, comprehension of "core competencies." and the terms and definitions contained in ATAP's "threat assessment glossary."[363]

Training is a critical need of personnel staffing fusion centers and according to the *Fusion Center Guidelines*:

> It is recommended that fusion centers adhere to the training objectives outlined in the *National Criminal Intelligence Sharing Plan (NCISP)*. In addition, it is recommended that personnel working within the center meet the core training standards developed by the Global Intelligence Working Group (GIWG) and Counter-Terrorism Training Coordination Working Group (CTTWG). Each of the six training classifications identified by the CIWG (intelligence analyst, intelligence supervisor, law enforcement officer, law enforcement executive, intelligence officer/collector, and train-the-trainer) have standards.[364]

Learning to conduct behavioral threat assessment and management is important to developing a capability for staff members within a fusion center to perform this work. However, it is also important for a fusion center to develop a structured process by which assessments and management activities will be performed. The need for these processes is in keeping with recommendations that fusion centers establish structured procedures regarding intelligence analysis.[365] Each fusion center may establish its own protocols pertaining to threat assessments and management cases within the general framework of guidance that already exists for fusion centers.

B. CHALLENGES AND OPPORTUNITIES—PREVENTION OF VIOLENCE

It has been suggested that the adoption of the all-hazards-all crimes mission by fusion centers is worth pursuing so long as the core fusion center responsibility of terrorism analysis can be sustained.[366] Since fusion centers are operated and managed at

[363] "Certified Threat Manager."

[364] Criminal Intelligence Coordinating Council, *Fusion Center Guidelines*, 53.

[365] Ibid., 21.

[366] Michael McCaul and Peter King, *Majority Staff Report on the National Network of Fusion Centers* (Washington, DC: The United States House of Representatives Committee on Homeland Security, 2013), 12.

the state and local level, balance is required to ensure that state and local needs are being met while also serving national priorities as they pertain to threat analysis and efforts to deal with terrorism.[367] Thus, in this scenario, the needs of state and local agencies may be served by fusion centers performing behavioral threat assessment and management services. The case examples offered earlier demonstrate how it may occur.

Looking beyond the immediate training needs of fusion centers or their state and local priorities, long-term opportunities also exist for fusion centers to apply behavioral threat management programs to address persistently vexing problems with a national nexus, particularly the phenomenon of violent extremism in the United States. Studies of extremist violence have led to the conclusion that definitive or valuable profiles of would-be attackers do not exist.[368] Further, Rutgers University Professor John Cohen reports that most violent extremists studied in the United States are "self-radicalized, self-trained, self-executing, and ideologically ignorant."[369] Professor Cohen goes on to note that while useful profiles of violent attackers are lacking, behavioral and psychological commonalities do exist.[370] These behaviors, when placed into appropriate context, may be analyzed for the purposes of proactive intervention in attack planning or execution.[371] The warning behaviors noted earlier, when analyzed within a behavioral threat assessment process, represent key opportunities to detect and disrupt potential incidents of terrorist violence.

Reactive tactical approaches, made by specialized police tactical teams to arrest key offenders or by military campaigns targeting individual terror leaders overseas, offer short-term solutions to combatting terrorism or crime because those targeted for arrest or assassination (in the case of overseas military actions) are merely replaced by others in

[367] McCaul and King, *Majority Staff Report on the National Network of Fusion Centers*, 13.

[368] John D. Cohen, "The Next Generation of Government CVE Strategies at Home: Expanding Opportunities for Intervention," *The Annals of the American Academy of Political and Social Science* 668, no. 1 (November 1, 2016): 119, doi: 10.1177/0002716216669933.

[369] Ibid.

[370] Ibid.

[371] Ibid., 124.

the same organizations.[372] The cycle of removing key leaders or operators through special tactics goes unbroken.

The preventive mission undertaken by fusion centers, and more broadly, the U.S. government, offers the greatest opportunity for a lasting strategy to mitigate terrorism and prevent violence.[373] Thus, fusion centers may support their federal, state, and local partners through the multi-disciplinary approaches to prevention by involving those who have the opportunities to observe people who may pose risks or harm to others.[374] Today, fusion centers are increasingly involved with the analysis of open-source social media posts. This sort of analysis does not require reams of classified data or secret informants because open-source data is growing at a rate that makes it exceedingly valuable.[375] Social media provides excellent real-time insights into events developing across the world or events occurring locally.[376] Much of the information of use to police agencies and fusion centers occurs in the open via social media posts.[377] An example occurred in in April 2015, days before two radicalized subjects attempted to attack an event in Garland, Texas known as a Prophet Muhammad cartoon contest.[378] The men, clad in body armor and armed with rifles, engaged traffic officers with gunfire after arriving at the perimeter of the event.[379] However, each attacker was shot and killed by the police officers with whom they exchanged gunfire.[380] Later, it was determined that one of the attackers had made several posts to his Twitter account that may have indicated an intent to attack the Garland, Texas event as the subject even used the hashtag "#texasattack."[381]

[372] Fathali M. Moghaddam, "The Staircase to Terrorism: A Psychological Exploration," *American Psychologist* 60, no. 2 (2005): 167, doi: 10.1037/0003-066X.60.2.161.

[373] Ibid.

[374] Cohen, "The Next Generation of Government CVE Strategies at Home," 124.

[375] Jane Harman, "Disrupting the Intelligence Community: America's Spy Agencies Need an Update," *Foreign Affairs* 2015, 105.

[376] Ibid., 106.

[377] Ibid.

[378] Scott Shane, "Texas Attacker Left Trail of Extremist Ideas on Twitter," *The New York Times*, May 5, 2015, http://www.nytimes.com/2015/05/06/world/middleeast/isis-texas-muhammad-cartoons.html.

[379] Ibid.

[380] Ibid.

[381] Ibid.

This post was among a larger number of social media posts that may have indicated his desire or intent to commit a violent attack in Garland, Texas.[382] One of the attackers began posting his affinity for ISIL approximately six months prior to the attack in 2015, which ultimately led the FBI to begin an investigation into him.[383]

Fusion centers and police agencies across the country are using a variety of services to help observe, digest, and add context to the huge volume of open-source social media posts made each day. These tools and their use by police departments and fusion centers have become the targets of critics, who often express concern regarding activities protected by the Fourth Amendment of the U.S. Constitution. It has been suggested that the use of tools that allow law enforcement to observe the posts that people make to social media is unacceptable and should be curtailed.[384] Following a complaint made by the American Civil Liberties Union, social media companies Facebook, Instagram, and Twitter withdrew their data feeds from a social media monitoring service called Geofeedia, which was frequently used by police agencies and fusion centers to detect the sort of social media posts noted previously as examples of the sorts of posts that may indicate imminent violence.[385]

Observation of social media is a real opportunity to detect *leakage, identification, pathway, fixation, last resort* and *directly communicated threat* warning behaviors.[386] The use of services that help to observe such posts are necessary due to the immense volume of data posted to social media each day. Fusion centers and others in the law enforcement arena must be proactive by developing policies that govern the proper use of social media analysis tools to ensure that privacy, civil rights, and civil liberties are protected.

[382] Shane, “Texas Attacker Left Trail of Extremist Ideas on Twitter.”

[383] Ibid.

[384] Elizabeth Dwoskin, “Police Are Spending Millions of Dollars to Monitor the Social Media of Protesters and Suspects,” *The Washington Post*, November 18, 2016, https://www.washingtonpost.com/news/the-switch/wp/2016/11/18/police-are-spending-millions-to-monitor-the-social-media-of-protesters-and-suspects/?utm_term=.7c824efdc554.

[385] Ibid.

[386] Meloy et al., “The Role of Warning Behaviors in Threat Assessment,” 265–266.

Adoption of a behavioral threat assessment and management capability in a fusion center requires collaborative relationships with a host of organizations that may contribute to an assessment or management strategy to prevent violent crime or terrorism.[387] Indeed, the prevailing objective of any fusion center should be the "movement from a reactive response to a proactive and preventive approach" that will improve the opportunities for police forces to prevent crime and terrorism but also to help the larger public safety community better prepared to respond after unwanted emergencies have occurred.[388] Making the case for prevention in 2005, Georgetown University professor Fathali Moghaddam observed, "prevention is the long-term solution," framing the significance of the issue by adding that policymakers in the United States "have no choice but to adopt a preventive approach to terrorism because the survival of the United States as a democratic superpower is at stake."[389] Dr. Moghaddam continued that repeated attacks against the United States would present significant damage to the America's economy, society, collective psychology, and political dynamic.[390] Such stakes compel forward action to prevent the violence so damaging to the nation.

Moving forward, the National Network of Fusion Centers continues to grow and mature. This maturity means that the core capabilities, which began to be tested by the DHS in 2011, have largely been achieved.[391] Today, baseline capabilities may now be taken for granted and the emerging emphasis for the network is to identify and develop new capabilities.[392] It is in this spirit that the discipline of behavioral threat assessment and management may find new practitioners within the nation's fusion centers as the need to identify threats, investigate them, and mitigate them continues.

[387] Criminal Intelligence Coordinating Council, *Fusion Center Guidelines*, 67.

[388] Ibid., 68.

[389] Moghaddam, "The Staircase to Terrorism," 167.

[390] Ibid.

[391] U.S. Department of Homeland Security, *2015 National Network of Fusion Centers—Final Report* (Washington, DC: U.S. Department of Homeland Security, 2016), 19.

[392] Ibid.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

110th Congress. *Implementing Recommendations of the 9/11 Commission Act of 2007*, 121 STAT. 266, 2007, 322. Washington, DC: Government Printing Office, 2007. https://www.nctc.gov/docs/ir-of-the-9-11-comm-act-of-2007.pdf.

Association of Threat Assessment Professionals. "About ATAP." 2013. http://www.atapworldwide.org/?page=1.

———. "ATAP Chapters." 2013. http://www.atapworldwide.org/?page=25.

———. "Certified Threat Manager." 2015. http://www.atapworldwide.org/default.asp?page=CTM.

Banks, Sandy. "'Cyber Banging' Drives New Generation of Gang Violence." *Los Angeles Times,* sec. Local/Crime & Courts, October 3, 2015. http://www.latimes.com/local/crime/la-me-1003-banks-lapd-gang-shootings-20151003-column.html.

Becker, Gavin De. *The Gift of Fear*. New York: Dell Publishing, 1997. Kindle edition.

Blair, John Peterson, and Katherine W. Schweit. "A Study of Active Shooter Incidents, 2000–2013." University of Colorado at Boulder, 2013. https://hazdoc.colorado.edu/handle/10590/2712.

Borum, Randy, Robert Fein, Bryan Vossekuil, and John Berglund. "Threat Assessment: Defining an Approach for Evaluating Risk for Targeted Violence." *Behavioral Sciences & the Law* 17, no. 3 (1999): 323–337.

Brannan, David, Kristin Darken, and Anders Strindberg. *A Practitioner's Way Forward*. Salinas, CA: Agile Press, 2014.

Bulling, Denise, and Mario Scalora. "Threat Assessment Glossary." 2013. http://digitalcommons.unl.edu/publicpolicypublications/123/.

Bush, George W. *National Strategy for Information Sharing: Successes and Challenges in Improving Terrorism-Related Information Sharing*. Bloomington, IN: Wordclay, 2009. http://books.google.com/books?hl=en&lr=&id=vEJbUn3nQ4cC&oi=fnd&pg=PA1&dq=%22the+sharing+of+information+across+all+levels+of+government,+disciplines,+and%22+%22Strategy+was+developed+with+the+understanding+that+homeland+security+information,%22+%22of+funding+and+other+resources+for+homeland+security-related%22+&ots=PJfoeP_WAO&sig=SBNmmgke3w5qtlMUd3IUyxHDdF0.

Cacialli, Douglas Owen. "Predicting Problematic Approach Behavior toward Politicians: Exploring the Potential Contributions of Control Theory." PhD diss., University of Nebraska-Lincoln, 2010. http://digitalcommons.unl.edu/psychdiss/23/.

Calhoun, Frederick S., and Stephen W. Weston. *A Practical Guide for Identifying, Assessing and Managing Individuals of Violent Intent*. San Diego, CA: Specialized Training Services, 2003.

Calhoun, Frederick, and Stephen Weston. *Contemporary Threat Management*. San Diego, CA: Specialized Training Services, 2003.

Carter, David L. *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies*, 2nd ed. Washington, DC: U.S. Department of Justice Office of Community Oriented Policing Services, January 2009. https://it.ojp.gov/documents/d/e050919201-IntelGuide_web.pdf.

Cohen, John D. "The Next Generation of Government CVE Strategies at Home: Expanding Opportunities for Intervention." *The Annals of the American Academy of Political and Social Science* 668, no. 1 (November 1, 2016): 118–128. doi: 10.1177/0002716216669933.

Cohen, Katie, Fredrick Johansson, Lisa Kaati, and Jonas Clausen Mork. "Detecting Linguistic Markers for Radical Violence in Social Media." *Terrorism and Political Violence* 26, no. 1 (January 2014): 246–256, doi: 10.1080/09546553.2014.849948.

Cornell, Dewey. *The Virginia Model for Student Threat Assessment*. Charlottesville, VA: University of Virginia, 2010. http://curry.virginia.edu/uploads/resourceLibrary/Virginia_Model_for_Student_Threat_Assessment_overview_paper_7-16-10.pdf.

Criminal Intelligence Coordinating Council. *Fusion Center Guidelines: Law Enforcement Intelligence, Public Safety, and the Private Sector.* Washington, DC: Criminal Intelligence Coordinating Council, 2006. https://it.ojp.gov/gist/94/Fusion-Center-Guidelines--Law-Enforcement-Intelligence--Public-Safety--and-the-Private-Sector.

Dahl, Erik. "Domestic Intelligence Today: More Security but Less Liberty?" *Homeland Security Affairs* 7, no. 2 (2011): 1–9. http://search.proquest.com/openview/710cc09449b7b0d18bd97395ee5ad261/1?pq-origsite=gscholar.

Deisinger, Gene, Marisa Randazzo, Daniel O'Neill, and Jenna Savage. *The Handbook for Campus Threat Assessment Teams*. Stoneham, MA: Applied Risk Management, LLC, 2008.

Depue, Roger L., and Susan Schindehette. *Between Good and Evil*. New York: Time Warner Group, 2005.

Dietz, Park E. "Mass, Serial and Sensational Homicides." *Bulletin of the New York Academy of Medicine* 62, no. 5 (1986): 477–491.

Dunn, Jeff. "Operations of the LAPD Threat Management Unit." *Stalking, Threatening, and Attacking Public Figures*, 2008.

———. "The Los Angeles Police Department Threat Management Unit." In *International Handbook of Threat Assessment*, edited by J. Reid Meloy and Jens Hoffmann, 285–298. New York: Oxford University Press, 2014.

Dwoskin, Elizabeth. "Police Are Spending Millions of Dollars to Monitor the Social Media of Protesters and Suspects." *The Washington Post*, November 18, 2016. https://www.washingtonpost.com/news/the-switch/wp/2016/11/18/police-are-spending-millions-to-monitor-the-social-media-of-protesters-and-suspects/?utm_term=.7c824efdc554.

Fein, Robert A. *Threat Assessment in Schools: A Guide to Managing Threatening Situations and to Creating Safe School Climates*. Collingdale, PA: Diane Publishing, 2002. http://books.google.com/books?hl=en&lr=&id=wHDt1OMyzUYC&oi=fnd&pg=PA9&dq=%22Center+have+found+that+some+school+attacks+may+be+preventable.%22+%22efforts+to+identify,+assess,+and+manage+students+who+may+have+the+intent%22+%22and+public%22+%22personnel,+issues+of+information+sharing,+and+ideas+for+creating%22+&ots=gsXdV5AVmQ&sig=5r1rLLywbCvMS9klbm398FUGKJA.

Fein, Robert A., and Bryan Vossekuil. *Protective Intelligence Threat Assessment Investigations*. Washington, DC: U.S. Department of Justice Office of Justice Programs, 1998.

Fein, Robert A., Bryan Vossekuil, and Gwen A. Holden. *Threat Assessment: An Approach to Prevent Targeted Violence*. Washington, DC: National Institute of Justice, 1995.

Grossman, Dave. *On Killing: The Psychological Cost of Learning to Kill in War and Society*. New York: Integrated Media Incorporated, 2014. Kindle edition.

Gruenewald, Jeff, William S. Parkin, Brent L. Smith, Steven M. Chermak, Joshua D. Freilich, Paxton Roberts, and Brent Klein. *Validation of the Nationwide Suspicious Activity Reporting (SAR) Initiative: Identifying Suspicious Activities from the Extremist Database (ECDB) and the American Terrorism Study (ATS)*, Report to the U.S. Department of Homeland Security. College Park, MD: National Consortium for the Study of Terrorism and Responses to Terrorism (START), 2015.

Guidetti, Ray. "Local Policing: Expanding Reach with Limited Resources through Fusion Centers." *The Police Chief*, February 2012.

Guns.com. "Russian/USSR Military AK-47." Accessed November 26, 2016. http://www.guns.com/reviews/russianussr-military-ak-47/.

Hafez, Mohammed, and Creighton Mullins. "The Radicalization Puzzle: A Theoretical Synthesis of Empirical Approaches to Homegrown Extremism." *Studies in Conflict & Terrorism* 38, no. 11 (November 2, 2015): 958–975. doi:10.1080/1057610X.2015.1051375.

Harman, Jane. "Disrupting the Intelligence Community: America's Spy Agencies Need an Update." *Foreign Affairs*, 2015.

Harris, Andrew J., and Arthur J. Lurigio. "Threat Assessment and Law Enforcement Practice." *Journal of Police Crisis Negotiations* 12, no. 1 (May 2012): 51–68. doi: 10.1080/15332586.2012.645375.

Hinman, Dayle L., and Patrick E. Cook. "A Multi-Disciplinary Approach to Threat Assessment." *Journal of Threat Assessment* 1, no. 1 (2001): 17–33.

Hoffman, Jens, J. Reid Meloy, and Lorraine Sheridan. "Contemporary Research on Stalking, Threatening, and Attacking Public Figures." In *International Handbook of Threat Assessment* edited by J. Reid Meloy and Jens Hoffmann, 160–177. New York: Oxford University Press, 2014.

Homeland Security Advisory Council. *Homeland Security Advisory Council Intelligence and Information Sharing Initiative—Final Report*. Washington, DC: U.S. Department of Homeland Security, 2004.

Hoover, Ryan, and Daniel Shaw. "How to Stop an Active Killer." *Small Wars Journal*, June 29, 2016.

Houston Mayor's Office of Public Safety and Homeland Security. "Run. Hide. Fight. Surviving an Active Shooter Event." Video, 2013. https://www.fbi.gov/about-us/cirg/active-shooter-and-mass-casualty-incidents/run-hide-fight-video.

International Association of Chiefs of Police. *Razing Expectations-Erecting a Strategic Vision for Fusion Centers*. Alexandria, VA: International Association of Chiefs of Police, 2009. http://www.theiacp.org/portals/0/pdfs/RazingExpectations.pdf.

Jaitner, Margarita. "Countering Threats: A Comprehensive Model for Utilization of Social Media for Security and Law Enforcement Authorities." *International Journal of Cyber Warfare and Terrorism* 4, no. 2 (April 2014): 35–45. doi: 10.4018/ijcwt.2014040103.

Jarvis, John, and J. Amber Scherer. *Mass Victimization-Promising Avenues for Prevention*. Washington, DC: Federal Bureau of Investigation, 2015.

Jenkins, Debra M. "The U.S. Marshals Service's Threat Analysis Program for the Protection of the Federal Judiciary." *The Annals of the American Academy of Political and Social Science* 576, no. 1 (2001): 69–77.

Kosinski, Michal, David Stillwell, and Thore Graepel. “Private Traits and Attributes Are Predictable from Digital Records of Human Behavior.” *Proceedings of the National Academy of Sciences of the United States of America* 110, no. 15 (April 9, 2013): 5802–5805.

Malone, Rick. “Protective Intelligence: Applying the Intelligence Cycle Model to Threat Assessment.” *Journal of Threat Assessment and Management* 2, no. 1 (March 2015): 53–62.

McCaul, Michael, and Peter King. *Majority Staff Report on the National Network of Fusion Centers*. Washington, DC: The United States House of Representatives Committee on Homeland Security, 2013.

Meloy, J. Reid. “Approaching and Attacking Public Figures: A Contemporary Analysis of Communications and Behavior.” *Journal of Threat Assessment and Management* 1, no. 4 (2014): 243–261. doi: 10.1037/tam0000024.

———. *Violence Risk and Threat Assessment*. San Diego, CA: Specialized Training Services, 2000.

Meloy, J. Reid, and Jens Hoffman. *International Handbook of Threat Assessment*. Oxford, New York: Oxford University Press, 2014.

Meloy, J. Reid, and Mary Ellen O’Toole. “The Concept of Leakage in Threat Assessment.” *Behavioral Sciences & the Law* 29, no. 4 (July 2011): 483–620. doi: 10.1002/bsl.986.

Meloy, J. Reid, Anthony G. Hempel, Kris Mohandie Andrew A. Shiva, M. Phil., B. Thomas Gray. “Offender and Offense Characteristics of a Nonrandom Sample of Adolescent Mass Murderers.” *Journal of the American Academy of Child & Adolescent Psychiatry* 40, no. 6 (June 2001): 719–728. doi: 10.1097/00004583-200106000-00018.

Meloy, J. Reid, Jens Hoffmann, Angela Guldimann, and David James. “The Role of Warning Behaviors in Threat Assessment: An Exploration and Suggested Typology: Warning Behaviors in Threat Assessment.” *Behavioral Sciences & the Law* 30, no. 3 (May 2012): 256–79. doi: 10.1002/bsl.999.

Miller, Anna. “Threat Assessment in Action.” *Monitor on Psychology* 45, no. 2 (February 2014): 37.

Moghaddam, Fathali M. “The Staircase to Terrorism: A Psychological Exploration.” *American Psychologist* 60, no. 2 (2005): 161–169. doi:10.1037/0003-066X. 60.2.161.

Mohandie, Kris, and James E. Duffy. “Understanding Subjects With Paranoid Schizophrenia.” *FBI Law Enforcement Bulletin* 68, no. 12 (1999): 8–16.

Monahan, Torin, and Neal A. Palmer. "The Emerging Politics of DHS Fusion Centers." *Security Dialogue* 40, no. 6 (December 1, 2009): 617–636. doi: 10.1177/096701 0609350314.

Mullen, Paul E., David V. James, J. Reid Meloy, Michele T. Pathe, Frank R. Farnham, Lulu Preston, Brian Darnley, and Jeremy Berman. "The Fixated and the Pursuit of Public Figures." *Journal of Forensic Psychiatry & Psychology* 20, no. 1 (February 2009): 1–15. doi: 10.1080/14789940802197074.

Mullins, Sam, and Adam Dolnik. "An Exploratory, Dynamic Application of Social Network Analysis for Modelling the Development of Islamist Terror-cells in the West." *Behavioral Sciences of Terrorism and Political Aggression* 2, no. 1 (January 2010): 3–29. doi: 10.1080/19434470903319441.

National Criminal Intelligence Resource Center. "Nationwide SAR Initiative (NSI)—About the NSI." Accessed July 24, 2016. https://nsi.ncirc.gov/about_nsi.aspx.

National Fusion Center Association. *National Strategy for the National Network of Fusion Centers*, 2014. https://nfcausa.org/html/National%20Strategy%20for%20the%20National%20Network%20of%20Fusion%20Centers.pdf.

Nationwide SAR Initiative. *Information Sharing Environment Functional Standard SAR 1.5.5* Washington, DC: Bureau of Justice Assistance, 2015. https://nsi.ncirc.gov/documents/SAR_FS_1.5.5_PMISE.pdf.

———. *Suspicious Activity Reporting Indicators and Examples*. Washington, DC: Nationwide SAR Initiative, 2015.

Odgers, Candice L., Edward P. Mulvey, Jennifer L. Skeem, William Gardner, Charles W. Lidz, and Carol Schubert. "Capturing the Ebb and Flow of Psychiatric Symptoms with Dynamical Systems Models." *American Journal of Psychiatry* 166, no. 5 (May 2009): 575–582. http://ajp.psychiatryonline.org/doi/abs/10.1176/appi.ajp.2008.08091398.

O'Toole, Mary Ellen, and Sharon S. Smith. "Fundamentals of Threat Assessment for Beginners." In *International Handbook of Threat Assessment*, edited by J. Reid Meloy and Jens Hoffmann, 272–282. New York: Oxford University Press, 2014.

Pang, Bo, and Lillian Lee. "Opinion Mining and Sentiment Analysis." *Foundations and Trends in Information Retrieval* 2, no. 1–2 (2008): 1–135. doi: 10.1561/1500000 001.

Patton, Desmond Upton, Robert D. Eschmann, and Dirk A. Butler. "Internet Banging: New Trends in Social Media, Gang Violence, Masculinity and Hip Hop." *Computers in Human Behavior* 29, no. 5 (September 2013): A54–A59. doi: 10.1016/j.chb.2012.12.035.

Pinker, Steven. *The Blank Slate-The Modern Denial of Human Nature*. New York: Penguin Putnam, Inc., 2002.

Randazzo, Marisa, and Ellen Plummer. *Implementing Behavioral Threat Assessment on Campus—A Virginia Tech Demonstration Project*. Blacksburg, VA: Virginia Polytechnic Institute and State University, 2009. https://www.threatassessment.vt.edu/Implementing_Behavioral_Threat_Assessment.pdf.

Scalora, Mario J., and William Zimmerman. “Then and Now: Tracking a Federal Agency’s Threat Assessment Activity through Two Decades with an Eye toward the Future.” *Journal of Threat Assessment and Management* 2, no. 3–4 (2015): 268–274. doi: 10.1037/tam0000057.

Schmalz, Dorothy, Craig Colistra, and Katherine Evans. “Social Media Sites as a Means of Coping with a Threatened Social Identity.” *Leisure Sciences* 37 (June 12, 2014): 20–38.

Shane, Scott. “Texas Attacker Left Trail of Extremist Ideas on Twitter.” *The New York Times*, May 5, 2015. http://www.nytimes.com/2015/05/06/world/middleeast/isis-texas-muhammad-cartoons.html.

Sigma Threat Management Associates. “Training.” Accessed November 16, 2016. http://www.sigmatma.com/law-enforcement-security/training/.

Simons, Andre, and Ronald Tunkel. “The Assessment of Anonymous Threatening Communications.” In *International Handbook of Threat Assessment*, edited by J. Reid Meloy and Jens Hoffmann, 195–213. New York: Oxford University Press, 2014.

Smith, Sharon S., Robert B. Woyach, and Mary Ellen O’Toole. “Threat Triage: Recognizing the Needle in the Haystack.” In *International Handbook of Threat Assessment*, edited by J. Reid Meloy and Jens Hoffmann, 321–329. New York: Oxford University Press, 2014.

Tobin. Chuck. “Message from the President: 25th Anniversary of the Association of Threat Assessment Professionals Annual Threat Management Conference.” *Journal of Threat Assessment and Management* 2, no. 3–4 (2015): 229–230. doi: 10.1037/tam0000053.

U.S. Department of Homeland Security. *2015 National Network of Fusion Centers—Final Report*. Washington, DC: U.S. Department of Homeland Security, 2016.

———. *Nationwide Suspicious Activity Reporting Initiative Concept of Operations*. Washington, DC: U.S. Department of Homeland Security, 2008. https://www.ise.gov/sites/default/files/NSI_CONOPS_Version_1_FINAL_2008-12-11_r1.0.pdf.

U.S. Department of Homeland Security and U.S. Department of Justice. *DHS/DOJ Fusion Process —Technical Assistance Program and Services*. Washington, DC: United States Government, 2014. https://www.ncirc.gov/documents/public/ Fusion_Process_catalog_of_services_version_8.pdf.

Uchida. Craig D. "The Development of the American Police." *Critical Issues in Policing: Contemporary Readings*, December 2004.

United States Department of Justice. *Baseline Capabilities for State and Major Urban Area Fusion Centers*. Washington, DC: United States Department of Justice, September 2008. http://it.ojp.gov/documents/d/baseline%20capabilities%20for%20state%20and%20major%20urban%20area%20fusion%20centers.pdf.

Virginia Fusion Center. *Information Report, Threat Assessment*. Richmond, VA: Virginia Fusion Center, April 29, 2016.

———. *Information Report, Threat Assessment*. Richmond, VA: Virginia Fusion Center, May 20, 2016.

———. *Information Report, Threat Assessment*. Richmond, VA: Virginia Fusion Center, November 14, 2016.

Virginia Law Library. "Threat Assessment Teams and Oversight Committees, Code of Virginia, vol. 22.1-79.4." 2013. http://law.lis.virginia.gov/vacode/title22.1/chapter 7/section22.1-79.4/.

Vossekuil, Bryan. *The Final Report and Findings of the Safe School Initiative: Implications for the Prevention of School Attacks in the United States.* Collingdale, PA: Diane Publishing, 2002. http://books.google.com/books?hl=en &lr=&id=YYrbptzXMMcC&oi=fnd&pg=PA1&dq=%22and,+%22What+can+be +done+to+prevent+future+attacks+from%22+%22out+school+attacks.+Particular +attention+was+given+to+identifying%22+%22creation+of+safe+environments+ for+students,+faculty,+and%22+&ots=pRvBcqY1JY&sig=HJTNTge0IOiEpH3N hv5IBBYs798.

Weiss, Michael, and Hassan Hassan. *ISIS—Inside the Army of Terror*. New York: Regan Arts, 2015.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California